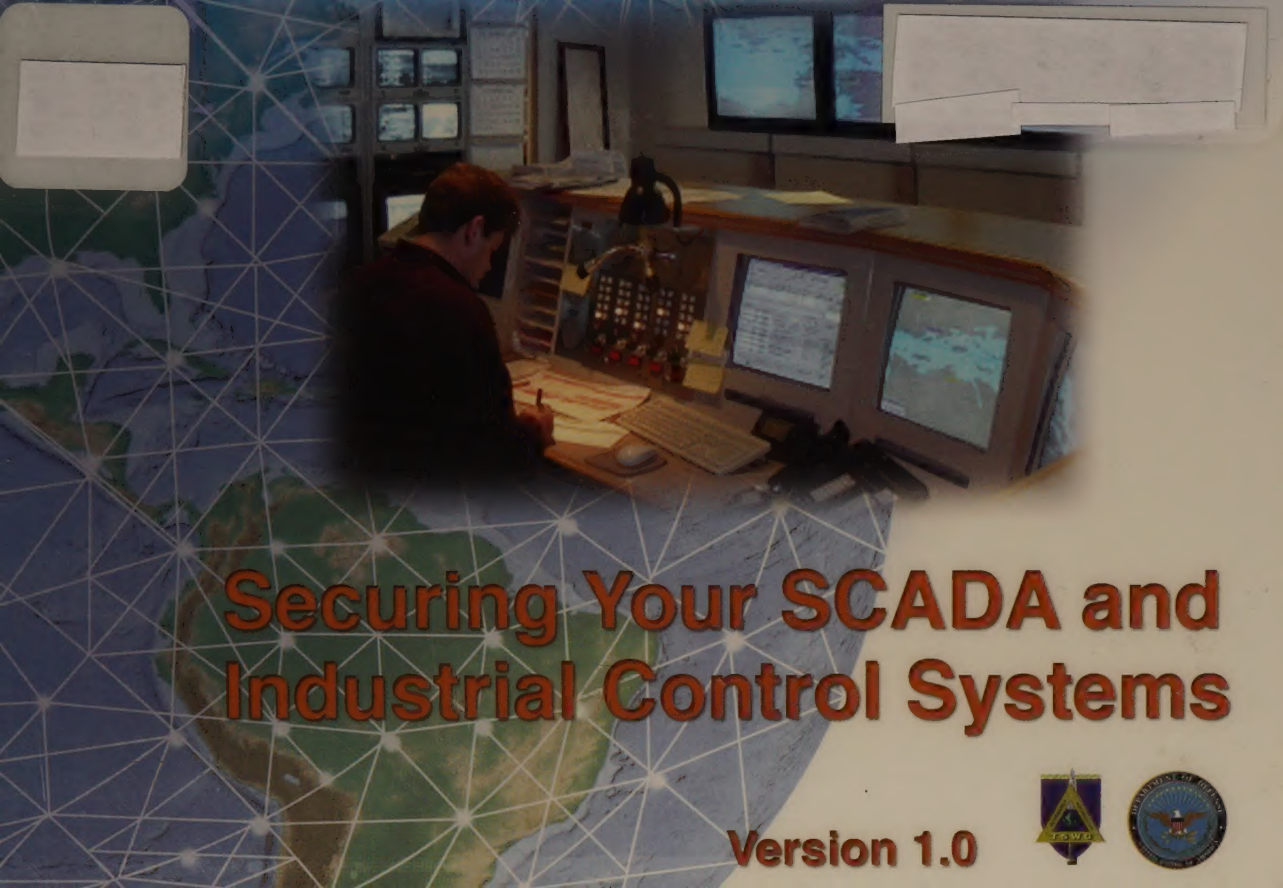


# Securing Your SCADA and Industrial Control Systems

Version 1.0

Additional copies of this guide are available from the Government Printing Office. To order, cite stock number 008-022-00338-0, ISBN 0-16-075115-8. Orders may be placed via the Internet, phone, fax, and mail.

For secure ordering via the Internet, visit the U.S. Government Online Bookstore at http://bookstore.gpo.gov.

Phone: (202) 512-1800
Monday through Friday, 7:30 a.m.-5:00 p.m., eastern standard time

Fax: (202) 512-2250 at any time

Mail: send to:
Superintendent of Documents
P.O. Box 371954
Pittsburgh, PA 15250-7954

All orders require prepayment, either by check, money order, VISA, MasterCard, Discover/NOVUS, or GPO Deposit Account.

(This page is intentionally left blank.)

# Disclaimer

The information in this guide is for informational purposes only and is not legal advice. The information is general and may or may not reflect the most current legal or technical developments. It does not constitute legal advice or substitute for obtaining legal advice from an attorney licensed in your state.

Copyright © 2005, Technical Support Working Group. All rights reserved.
Permission is granted to display, copy, publish, and distribute this document in its entirety, provided that the copies are not used for commercial advantage and that the present copyright notice is included in all copies, so that the recipients of such copies are equally bound to abide by the present conditions.

Unlimited release – Approved for public release.

# Purpose

This guidebook, developed by the Technical Support Working Group (TSWG), provides information for enhancing the security of Industrial Control Systems (ICS). The information is a comprehensive overview of industrial control system security, including administrative controls, architecture design, and security technology. This guide is intended for all sectors that use ICS technology. This is a guide for enhancing security, not a how-to manual for building an ICS, and its purpose is to teach ICS managers, administrators, operators, engineers, and other ICS staff what security concerns they should be taking into account.

# Scope

This guide does not constitute a standard, and it is not a substitute for standards documents. Neither is this guide a comprehensive security manual. It does not go into detail about any specific technologies; it covers ICS security too broadly to be used as a standalone document. Standards and vendor documents should be consulted for help in properly securing a specific ICS configuration.

# To Whom This Guide Applies

ICS is one term for a broader set of control systems, which include

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Digital Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- Any other automated control system

Each industry has its own culture and set of terms. This guide is useful for any industry employing networked automation systems, regardless of the terms used.

# Table of Contents


**1. Start Here** 1
- Disclaimer 1
- Purpose 2
- Scope 2
- To Whom This Guide Applies 2
- Table of Contents 3
- How to Use This Guidebook 7
- A Note on Anecdotes 7
- Guidebook User Roles 8
- Icons 9
- How to Use Frequently Requested Help 10
- Frequently Requested Help 10

**2. Setting the Foundation** 12
- Sustainable Security 13
- Effective Security Documentation 14
- Enforcement 15
- The Secure Design Process 16
- Secure Implementation 17
- Legal Obligations of Critical Infrastructure 18
- Critical Infrastructure Liability 19

**3. The Secure Design Process** 20
- The Secure Design Process Introduction 22
- Identify 23
- Object-Role Modeling 24
- ICS Reference Model 26
  - o How to Use 28
  - o General Types of Functionality 28
- External Entities 29
- Architecture and Design Suggestions 30
- Determine Adversarial Threat Models and Consequences of Concern 31
  - o Capabilities and Motivation to Initiate an Attack 32
- Data Types and Categories 33
  - o Data Protection 34
- Data Classification 35
- Risk Assessment 36

**4. Security Documentation** 40
- Security Documentation Introduction 41
- Documentation Relationships 42
- Types of Security Documentation 43
- Security Plan Elements 45
- Implementation Guidance 46

# Table of Contents (cont.)


**5. Policy** 47

- Policy Introduction 49
- How to Write Policy 49
- What Goes into a Policy? 50
- ICS Security Policy Framework 52
  - o ICS Security Program 54
  - o Data Security Policy 56
  - o Platform Security Policy 57
  - o Communication Security Policy 58
  - o Personnel Security Policy 60
  - o Configuration Management Policy 61
  - o Audit Policy 62
  - o Application Policy 64
  - o Physical Security Policy 65
  - o Manual Operations Policy 66

**6. Enforcement** 67

- Enforcement Introduction 69
- The Enforcement Cycle 69
- Aspects of Enforcement 70
- Configuration Management 71
  - o Why is Configuration Management Necessary? 71
  - o Configuration Management: Step 1 72
  - o Configuration Management: Step 2 73
  - o Configuration Management: Step 3 73
- Changes 74
  - o Change Request/Approval Process 74
- Test Labs 75
  - o Essential Elements of a Test Lab 76
- Auditing Versus Assessment 77
- Types of Audit and Assessment 78
- Steps for Using Audit and Assessment Results 79
- What to Look for in an Assessment Company 80

**7. ICS Best Practices** **81**
- Defense in Depth 83
- Security Program Best Practices 83
- Policy Best Practices 84
- Organizational Best Practices 84
- Data Security 85
- Malicious Software Protection 85
- Platform Security 86
- Security for RTUs, PLCs, or IEDs 88
- Communication Security 88
- Wireless Security 89
- Virtual Private Networks 89
- Firewalls 90
- Demilitarized Zones 91
- Proxies 91
- Remote Access 92
- External or Third Party Access 93
- Remote Access Servers (RAS) 94
- Personnel Security 94
- Accounts and Passwords 95
- Training 96
  - o What to Look for In a Training Class 96
- Assessment 97
- Auditing 97
- Intrusion Detection Systems 98
- Intrusion Prevention Systems 99
- Logging 99
- Applications 100
- Manual Operations 100
- Physical Protection 101
- Physical Asset Disposal 103
- Other Security Suggestions 104

**8. Finding Your Vulnerabilities** **105**
- Vulnerabilities and Threats 107
- ICS Security 108
  - o Historical ICS Security 108
  - o Current Issues 108
  - o Security Limitations of Legacy Equipment 108
- Poor ICS Practices 109
  - o Poor Account Maintenance 109
  - o Unprotected Network Connections 109
  - o Poor Application Implementation 109
  - o Lack of Maintenance and Monitoring 110
- Lack of ICS Security Documentation and Enforcement 110
- Lack of Physical Controls 111
- Inadequate Physical Protection of Equipment 112
- Remote Access 112
- Types of Remote Access 113
- Lack of Data Categorization and Sensitivity Guidance 114
- Protocol Vulnerabilities 114

# Table of Contents (cont.)

**9. Incident Handling and Response** 115
- How to Recover When Something Goes Wrong 116
- Incident Handling 117
- The Incident Handling Process 118
- After The Fact 119
- Indications of Incidents 120
- What to Do About Unusual Activity 120
  - o Malicious Code Resources 121
  - o Hoax Investigation Sites 121
  - o Detection and Recovery Sites 121
- Digital Forensics 122
- Threat Response 124

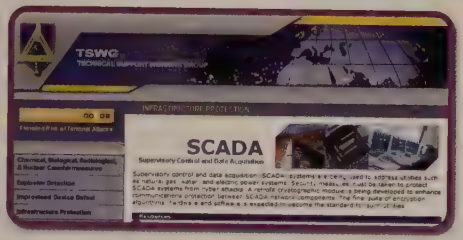
**10. Resources and References** 125
- References for each section 125
  - o Section 1 125
  - o Section 2 126
  - o Section 3 127
  - o Section 4 127
  - o Section 5 128
  - o Section 6 128
  - o Section 7 129
  - o Section 8 130
  - o Section 9 130
- Resources 132
- Definitions 135
- Acronyms 141
- Standards and Association Links 145
- ICS Primer 150
  - o Two Categories of ICS 150
  - o Manufacturing or Chemical 151
  - o Electric Power, Oil and Gas, and Water 151
  - o Automation Systems in Electric Power 152
- Related Works in Progress 153

## How to Use This Guidebook

This guide provides a foundation to help implement secure systems, secure existing systems, and make security a process rather than an afterthought. Working knowledge of ICS and basic cyber security is assumed.

Small colored boxes appear on the right-hand side of any page that implicitly refers to another section of the guide. Each such box contains the name of the section referred to and is that section's color.

The related TSWG website, http://www.tswg.gov/tswg/ip/scada.htm, contains more detailed information, updates, and job aids. Job aids include examples, templates, and references. A training support package will also be available with more detailed information for each section of the guide.




## A Note on Anecdotes

Many sections in this guide begin with short anecdotes. These anecdotes provide examples of actual ICS security incidents, and are meant to demonstrate potential consequences of inadequate security practices. The anecdotes are in italic font with colored backgrounds for easy recognition.

## Guidebook User Roles

This guide was written for a wide range of ICS staff. The roles defined below need not correlate perfectly with actual positions at a given ICS; they are meant to encapsulate job functions that must be performed by ICS staff in general. The icons appear at the beginning of each section, denoting the roles most applicable. All ICS staff, however, will benefit from reading each section.

Engineer/Tech

ICS Engineer/Technician – Designs and maintains the ICS; participates in testing and designing security response guidelines (e.g. manual operations, incident response); maintains the system hardware.

Operator

ICS Operator – Maintains the day-to-day operations of the ICS; and administers users' accounts and applications.

Security Admin

ICS Security Administrator – Maintains security documentation; oversees the implementation of all security controls; evaluates and implements the results of security audits and assessments; investigates security incidents; and administers users' accounts and application security.

ISO

ICS Information Security Officer – Maintains all data contained in the system, and ensures that security controls are adequate for the protection of data.

Manager

ICS Manager – Approves all changes to the ICS, including exceptions to policy, purchases, new equipment, acquisitions, and ensures all security requirements are met.

## Icons

The following icons are used throughout the guidebook to indicate other documents promoting the same recommendations, or cases where the TSWG website contains more detailed information.

**http://** See TSWG website for more information
http://www.tswg.gov/tswg/ip/scada.htm

**21** See "21 Steps to Improve Cyber Security of SCADA Networks"
http://www.tswg.gov/tswg/ip/21_Steps_SCADA.pdf

**NERC** See "NERC Critical Infrastructure Protection Standards CIP-002-1 through CIP-009-1"
http://www.nerc.com/~filez/standards-cyber.html
http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

**AGA-12** See "AGA-12: Cryptographic Protection of SCADA Communications General Recommendations"
http://www.gastechnology.org/webroot/downloads/en/1ResearchCap/1_1GasOps/AGASCADANews.pdf

**NRC** See "NRC: Criteria for use of Computers in Safety Systems of Nuclear Power Plants"
http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-152/

**API** See API's "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries" and "Security Guidelines for the Petroleum Industry"
http://www.npra.org/publications/general/SVA_2nd_Edition.pdf

## How to Use Frequently Requested Help

The Frequently Requested Help section lists common scenarios ICS engineers encounter that may require security knowledge and solutions. The list includes the page numbers of this guidebook that will assist the engineer in solving these problems with security in mind.

Not all issues can be covered by this guide. Every attempt has been made to cite the proper references where applicable.

## Frequently Requested Help


Responding to:
- An Incident **115-124**
  - Cyber Attack **118-119**
  - Forensic Analysis **122-123**
  - Observed Unusual Activity or Incident **120**
- A Threat **124**

New Regulations **18-19**, 42

Security-Related Upgrade Decisions **17**, **22-23**, **30-39**, [illegible]

Need an Audit/Assessment?: 80, [illegible]
- What Type of Audit/Assessment Do You Need? 78
- Why Audit/Assess? 62-63, 77
- System Benchmarking 72-73
- Using the Results of an Audit/Assessment 42, 79

Need to Write Documentation? **14**, 40-46
- Security Policy **43**, **47-66**
- Security Plan 44, 45
- Incident Response Guide 43, **116**
- Configuration Management Plan **43**, **71-73**

## Frequently Requested Help (cont.)


Need to Know If Something's Secure? [illegible]
- Evaluate the Security of a Design **24-28, 38-39**
- Select a Security Product 81-104

Need Implementation Help? [illegible]
- Security **22-30,** [illegible]
- Add-On Security Device 90-92

Best Practices for:
- Network Connections 90-95
- Communication Interfaces 89
- Monitoring Tools 99-100
- Using Equipment **87-92**
- Changing Equipment 74-76

How to Manage:
- Equipment Failure 66, 101
- Data Loss **33-35,** 56, 86
- Using Equipment with Security 46, [illegible]
- Changing Equipment 74-76

Where to Find More Information on:
- Regulations [illegible]
- Training 97
- User Groups [illegible]
- Government Standards 132-134

# Setting the Foundation

**Who:**

Manager

Engineer/Tech

Security Admin

Operator

**Why:** Security is necessary to maintain reliability of industrial control systems. Without security, the ICS and the organization's business are vulnerable to disruption through attack. A disruption in operation of an ICS may lead to legal action, worker injury, loss in revenue, loss of public trust, or even physical damage to the system being controlled by the ICS.

This section identifies and defines the critical elements of a sustainable security program and introduces other considerations that affect the security posture of an organization. Later sections detail how to create and implement the elements presented here.

**What:** Sustainable Security
Effective Security Documentation
Enforcement
The Secure Design Process
Secure Implementation
Legal Obligations of Critical Infrastructure
Critical Infrastructure Liability

## Sustainable Security

To have confidence in the security of any system, a culture of security must be developed and adopted by the organization. This culture of sustainable security is created through people, practices, procedures, and enforcement. If any one of these elements fails to consider security as a priority, the system will be weakened.

Key Elements

- Security Administration
  - o Effective security documentation
    - Policy
    - Plans
    - Procedures
  - o Enforcement
    - Consequences
    - Executive Support
    - Buy-in
- Security Technology
  - o Secure design
    - Building a system with security in mind
  - o Secure implementation
    - Equipment
    - Procedures

See Documentation

See Enforcement

See Secure Design

See Best Practices

# Effective Security Documentation

The first step in creating a sustainable security culture is to tie security objectives to the business goals of the organization. This practice turns security into a necessary system feature as opposed to an add-on. Security is inherently tied to reliability: if a system can be infiltrated, then all data reported by the system are questionable, and operators may not be able to maintain control.

Security documentation

- An **ICS security policy** translates security and reliability objectives into a set of rules and expected behaviors for system users.

- A **security plan** documents the process of planning and maintaining adequate, cost-effective security protection for a system.
- **Implementation guidance** is a set of directives for the installation, configuration, and maintenance of specific technologies.

- **Procedures** document appropriate behavior for repeatable situations. Incident response procedures and evacuation procedures, are examples of typical procedures needed by ICS. Implementation guides are a subset of procedure documents.

# Enforcement

Without enforcement, security documentation is not effective.

Buy-in

- All users of the system, including management, must believe that security is an important goal for the organization. Management can instill this attitude by following secure practices themselves, and by endorsing security awareness efforts within the organization.

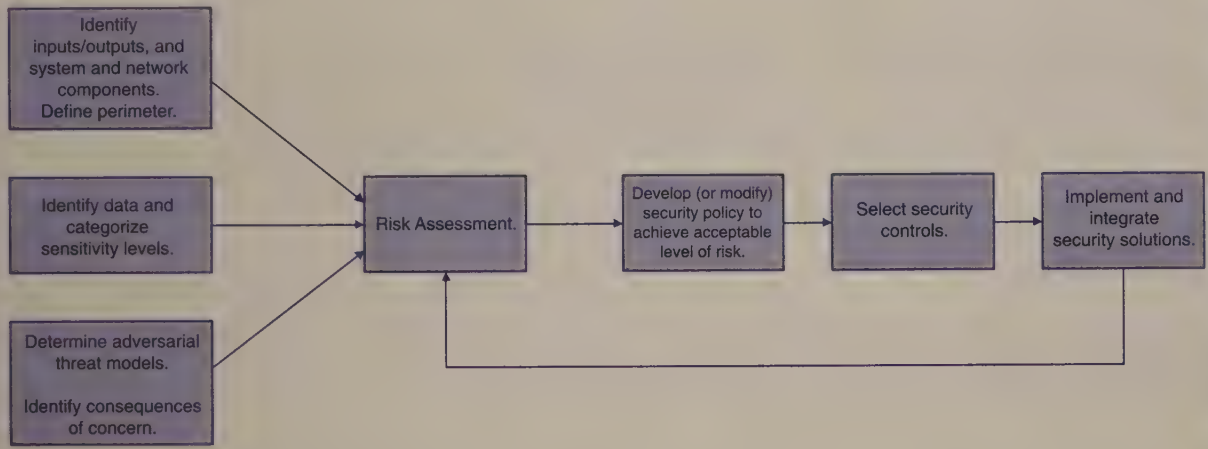
See Enforcement

Enforcement Elements

- Dedicated security administrators assigned specifically to the ICS.
- Effective configuration management.
- Auditing, both by internal staff members and external organizations, to ensure compliance with security controls.
- Third-party assessment of administration and implementation.
- Enforcement rules are consistently followed.
- Incident response procedures.

## The Secure Design Process

The secure design process is a step-by-step guide for designing or redesigning an ICS with security in mind. The process provides a broad overview that explains how to create and maintain a secure ICS network. The process is carefully ordered so that each step requires no additional information other than what was learned in previous steps.



## Secure Implementation

The most advanced security equipment is useless if not correctly implemented. Following best practices for secure implementation allows systems to benefit from the knowledge and experience of others.

See Best Practices

Best practices for secure implementation deal with configuration issues, organizational issues, policy, data security, platform security, and communication security, as well as proper use of network security tools.

Best practices for physical security are also important; physical and cyber security are tightly integrated in critical infrastructure.

- If possible, create a physical security monitoring system that is independent of the ICS in order to avoid a single point of failure.
- If you cannot afford a separate physical security system, you lose a valuable source of independent corroboration and probably create a super-user that knows both systems intimately.

# Legal Obligations of Critical Infrastructure

The federal government and state governments are becoming more aware of cyber and critical infrastructure security concerns and have enacted supporting legislation to protect information.

- Federal cyber security legislation
  - o HIPAA (Health Insurance Portability and Accountability Act of 1996)
- Information security requirements for the health industry
  - o Gramm-Leach-Bliley Act
- Information security requirements for the financial industry
  - o FISMA (Federal Information Security Management Act of 2002)
- Information security requirements for federal agencies
- State cyber security legislation
  - o California Senate Bill 1386
    - Companies must inform customers when their personal information is believed to have been compromised.
- National Strategy to Secure Cyber Space and National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
  - o Critical infrastructure has obligations to customers and the country.

## Critical Infrastructure Liability

- Failure to provide reasonable security measures to mitigate vulnerabilities could breach the "security duty of care" specified by the National Strategy to Secure Cyberspace and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and may be a cause of action for damages under tort law. Court opinions provide little precedent in this matter, and the potential limitations on critical infrastructure (CI) liability for downstream harm from cascading impact are unclear. The extent to which Gramm-Leach-Bliley might apply is unknown as well.

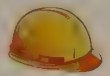
- Due diligence is not measured by any absolute standard, but depends upon the relative facts of a specific case.

- The Freedom of Information Act (FOIA) has been changed by the Homeland Security Act of 2002. Under the new provisions, critical infrastructure owners and operators may provide security-related information to the Department of Homeland Security without worry that such information will be subject to FOIA disclosure.

# The Secure Design Process

**Who:**

ISO



Engineer/Tech

**Why:** Secure design is critical for creating sustainable and reliable systems. Systems designed with security in mind are less vulnerable to attacks and prone to recover from problems both quickly and gracefully.

**What:**

- The Secure Design Process Introduction
- Identify
- Object-Roll Modeling
- ICS Reference Model
- How to Use
- General Types of Functionality
- External Entities
- Architecture and Design Suggestions
- Determine Adversarial Threat Models and Consequences of Concern
- Capabilities and Motivation to Initiate an Attack (From AGA-12)
- Data Types and Categories
- Data Protection
- Data Classification
- Risk Assessment

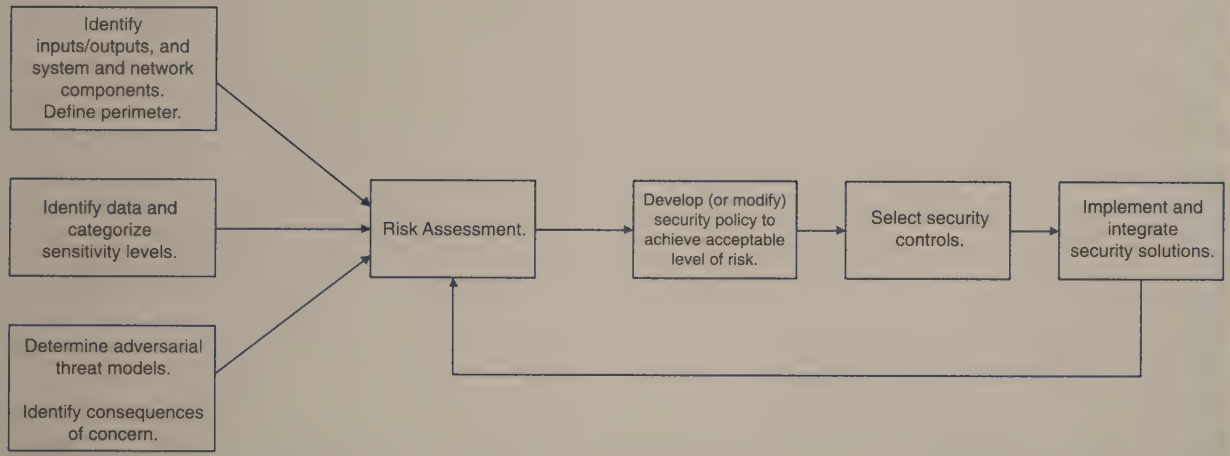
*The two most widely publicized critical infrastructure failures in recent memory, the August 2003 Northeast blackout and the September 2004 air traffic control system failure in southern California, resulted partially from computer software failures. According to the US-Canada Power System Outage Task Force, the blackout was largely the result of a malfunction in the Alarm and Event Processing Routine (AEPR) at a FirstEnergy power plant in Ohio. Further investigation showed that the failure of AEPR, an application designed by General Electric to alert operators of problems in the power system, was caused by a specific type of software bug called a "race condition," that result from poor programming.*

*The 2004 air traffic control failure, that left 800 planes in the air without contact for three hours, was the result of a bug in a Microsoft Windows-based system that the FAA phased in three years earlier. The system experienced data overload if it ran too long, and the servers were configured to automatically shut down if not rebooted in 49.7 days. When one improperly trained employee failed to reboot the servers, the system powered off, effectively shutting down air travel over all of southern California, including Los Angeles. The outage caused 400 flights to be delayed, 600 flights to be cancelled, and five incidents where planes flew closer than rules allow.*

*Both incidents could have been mitigated by proper configuration management, testing, and more rigorous employee training techniques. Both resulted, at least partially, from software glitches that should not have been present in an active critical infrastructure system, and that would not have been present had proper testing and code audits been completed prior to deployment.*

# The Secure Design Process Introduction

The secure design process is a step-by-step guide for designing or redesigning an ICS with security in mind. The process provides a broad overview explaining how to create and maintain a secure ICS. The process is carefully ordered so that each step should require no information other than what has been learned in previous steps.



# Identify

Before security controls can be put in place, system and network administrators must determine what controls are necessary. This means determining exactly what data must be allowed into and out of the network, where the network's perimeter lies, how the network is divided into security zones, and which components need special protection.

The first step in implementing security controls is to identify the functions that will be performed (or are performed) in the system. Next, the system itself must be defined.

Identify functions

- Identify owners of the total system.
- Develop functional system model.

Define system

- Identify boundaries and interfaces.
- Define inputs, outputs, and transformations.

# Object-Role Modeling

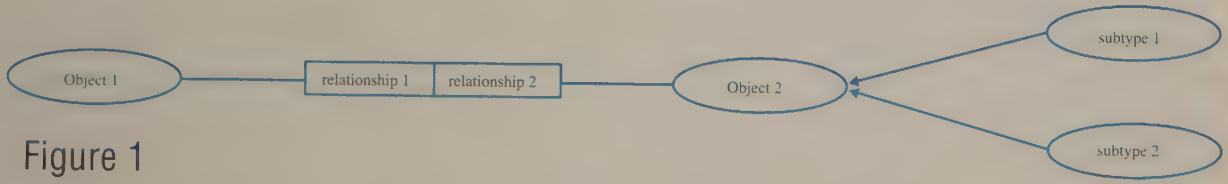


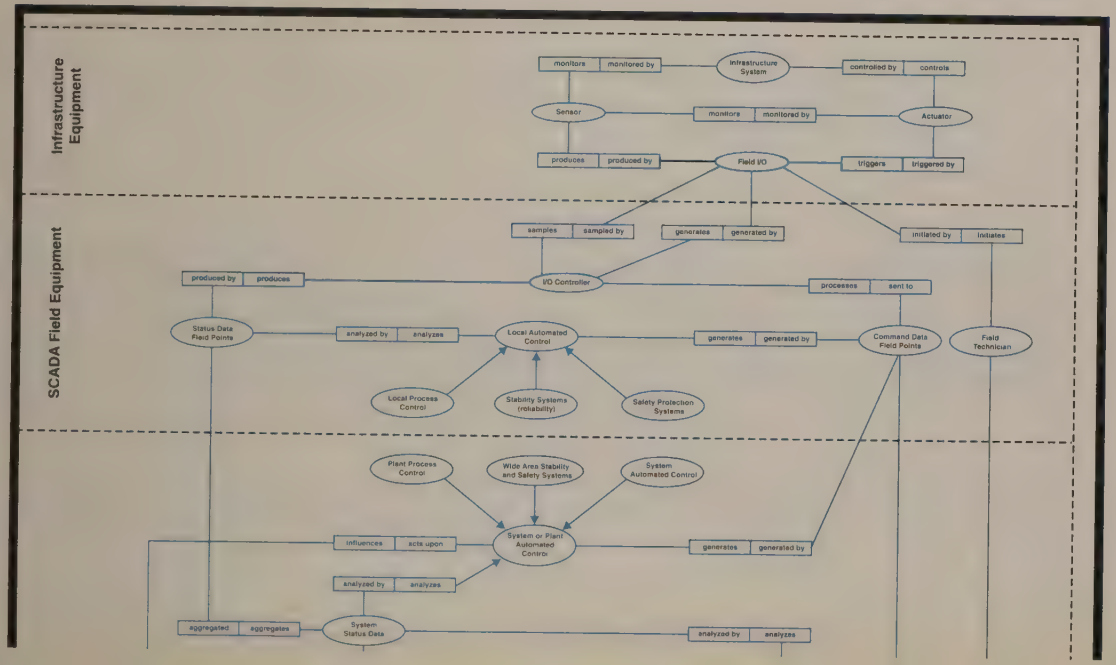

Figure 1

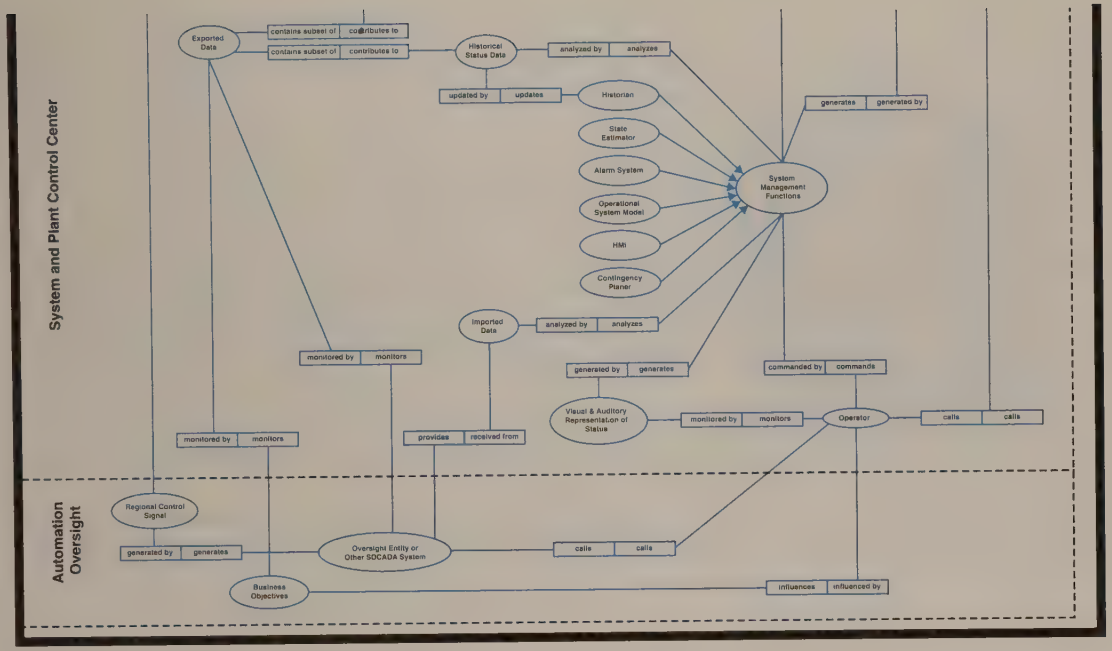
In object-role modeling, objects or ***entity types*** are represented as ovals. Roles are represented as boxes and annotate relationships between objects. Referring to Figure 1, the role is read as ***Object 1 has relationship 1 to Object 2*** and ***Object 2 has relationship 2 to Object 1***. Subtype relationships are represented as arrows. For example, ***Object 2*** has subtypes of ***subtype 1*** and ***subtype 2***. Similarly, ***subtype 1*** is one type of ***Object 2***, and ***subtype 2*** is another type of ***Object 2***. Objects in the model are types or classes, and there is frequently more than one instance of an object type in a system. An object in the model serves as a reference for features and properties that are common across all instances of that object within the system.

The ICS Reference Model on the following two pages illustrates the use of object-role modeling to represent the elements and functions of a generic ICS. The ICS Reference Manual is available as a separate PDF file on the TSWG website. http://www.tswg.gov/tswg/ip/scada.htm

(This Page Intentionally Left Blank)

# ICS Reference Model




System and Plant Control Center
Automation Oversight
Exported Data
contains subset of
contributes to
contains subset of
contributes to
Historical Status Data
analyzed by
analyzes
updated by
updates
Historian
State Estimator
Alarm System
Operational System Model
HMI
Contingency Planer
System Management Functions
generates
generated by
Imported Data
analyzed by
analyzes
monitored by
monitors
generated by
generates
commanded by
commands
Visual & Auditory Representation of Status
monitored by
monitors
Operator
calls
calls
monitored by
monitors
provides
received from
Regional Control Signal
generated by
generates
Oversight Entity or Other SOCADA System
calls
calls
Business Objectives
influences
influenced by

## How to Use

Not every object and role in the model will be present in every industrial control system. For example, a small, independent manufacturing system is not likely to require the same type of real-time coordination and regional oversight as electric power distribution.

With this consideration in mind, when designing for security, the model can be applied to identify important categories of data, equipment, activities, and properties within the system.

Each piece of equipment should map to one or more of the bubbles in the ICS Reference Model.

## General Types of Functionality

- Local automated controls
- System or plant automated controls
- System management functions
- Connections to oversight entities or other ICSs

## External Entities

The operation of infrastructures has changed from something of a public service to more of a business. As such, many data sharing requirements and hierarchical relationships have been added to the ICS model.

- Business objectives
  - These include cost of inputs, processing, distribution, sale price, and contractual obligations.
- Oversight entity or another ICS
  - Examples in electric utilities include ISOs, RTOs, PXs, or other ICSs within a control area. Other industries may be linked to factories and inter-utility oversight functions.
- Regional control signal
  - These are generated by an oversight entity or another ICS to affect automated control across multiple ICSs.

Each external entity represents a point of entry into the system, and each must be examined to ensure that proper security mechanisms are in place to protect its interface.

# Architecture and Design Suggestions

- Mature policy and governance is essential.
- Control and data hierarchy
  - o Eliminate global access/privilege requirements.
  - o Use principle of least privilege.
  - o Set access level commensurate to level of data sensitivity.
- Interconnections
  - o Control direct connections through the perimeter.
  - o Ensure security enclaves are never violated.
- Evolution
  - o Perform risk assessment when adding new functions.
- Heterogeneity
  - o Diversity implementations to improve survivability.
  - o Increases cost, which must be balanced against security gains.
- Situational and operational security awareness
  - o Operators/personnel are aware of security issues.
  - o Conduct training.
- Redundancy
  - o Continuity of operations.
  - o Backups for critical data.
  - o Backups for critical communications.
  - o Backup platforms for critical nodes.

# Determine Adversarial Threat Models and Consequences of Concern

Because different adversaries have different resources, capabilities, and motivations, each adversary will attack in a different way and with a different goal. The ICS management team must decide which adversaries and potential consequences are most threatening to its specific system based on each adversary's likelihood of attack and the expected damage of each attack. For some systems, denial of service might be the worst possible consequence, and in such systems security features (e.g., Intrusion Prevention Systems) that have a tendency to cause denial of service should be disabled. For other systems, the worst possible consequence might be for classified information to fall into terrorist hands, and in those cases data security should be given the highest priority. Secure design necessarily involves tradeoffs: no system is perfectly secure, and each security mechanism presents new security and reliability concerns. Knowing what to defend against is the key to making sound decisions with regard to security and reliability priorities. The table on the next page lists the capabilities, resources, and motivations of common adversaries.

## Capabilities and Motivation to Initiate an Attack (From AGA-12)

| Attacker/threat agent | Special capabilities/resources | Motivation |
|---|---|---|
| Hackers | Computer, spare time, dedication | Fun, challenge, fame |
| Organized crime | Computer skill | Financial gain |
| Traders | Computer skill | Financial gain |
| Extremists | Computer skill, dedication | Harm groups they oppose |
| Terrorists | Computer skill, spying, money, organization | Terrorize, finance operations, economic damage |
| Foreign governments | ICS expertise, large computers, cryptographers, intelligence agency, money, military | Strategic military and/or economic damage |
| Insiders, contractors | System access, confidential information | Revenge, union issue, grievance |
| Alliances of above groups | Combined resources of any above group | Alliance of convenience to advance own interest |

## Data Types and Categories

Each data type and category must be protected according to its criticality within the system. After the data types have been identified, the category of each type should be determined.

Data Types

- Hardware and software configurations
- Sensor readings
- Control messages (to actuators, sensors, etc.)
- Passwords and usernames
- Historical data

Data Categories

- Field I/O
- Status data field points
- Command data field points
- System status data
- Historical status data
- Imported status data
- Exported status data
- Regional control signals

# Data Protection

NERC

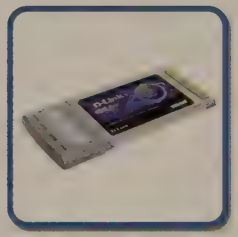
Protect data in all forms and during all operational conditions.

Forms of data

- Voice
- Electronic Data
  - o Fax
  - o Wired network
  - o Wireless network
- Removable media
- Print media

Operational conditions

- Normal
- Maintenance/construction
- Database retrieval
- Software installation and updates



## Data Classification

All data will not need the same level of protection. Dividing data into different classifications allows an organization to determine protection levels.

Some examples of classifications

- For private companies
  - o Public data - Data is not sensitive; release of this information poses no threat.
  - o Company confidential data - Release could damage the company.
- For critical infrastructure under DoD
  - o For Official Use Only (FOUO) - Unclassified information exempt from public release and restricted to need-to-know (NTK) access.
  - o Classified - Data should not be released outside of the organization; release could result in harm to the organization (and could harm national security).

# Risk Assessment

A systematic risk assessment will result in a list of vulnerabilities, as well as a quantitative ranking of the consequences resulting from successful exploitation of each vulnerability. Risk assessment is a critical step in designing security; it identifies and prioritizes vulnerabilities, thereby allowing an organization to determine acceptable mitigation strategies.

Risk assessment steps

- Identify assets and consequences of concern.
- Identify adversary (skills, motivation).
- Develop scenarios in which the adversary can cause consequences of concern.
- Prioritize risk and evaluate success factors.
- Evaluate current effectiveness in preventing attacks.
- Develop further mitigation to prevent attacks.
- Prioritize mitigation strategy and set timetables for implementations.

API

Risk assessments can be considered in terms of their approach and the personnel intended to execute them. For the latter, risk assessment methods can be designed for experienced assessors, inexperienced owners of assets, or somewhere in between. The approach can be comparative, temporal, or functional.

Comparative methodology:

1. Compare security practices and procedures for automation systems to relevant industry best practice.

This method is the simplest to execute, but it is dependent on the experience and capability of the assessor to best relate the security practices with the actual implementation of the automation systems.

Temporal methodology:

1. Develop a team that can act as a hypothetical adversary.
2. Assign measures of success to the adversary team.
3. Allow the adversarial team to engage the automation systems (actually, preferably a model thereof for purposes of safety).

This method allows the greatest fidelity, but also may have a narrow focus.

## Risk Assessment (cont.)

Functional methodology:

1. Identify critical operations or procedures that depend on automation systems.
2. Determine the potential impacts to operations assuming malfunctioning automation systems.
3. Consider the likelihood of various modes of automation malfunction:
    a. Determine the vulnerability of the automation systems and their constituent elements to attacks causing malfunction, and
    b. To the extent possible, consider the probability that an adversary exists that has the motivation and capability to execute these attacks.
4. Based on Step 3 above, rank vulnerability/impact combinations based on the expected risk.
5. Develop a mitigation strategy that best safeguards the correct operation of automation systems.

This method tries to combine the breadth of the comparative methods with the depth of the temporal. However, this method also relies heavily on experience and analysis, particularly in steps 3) and 4).

For more information, please refer to "A Classification Scheme for Risk Assessment Methods," (SAND 2004-4233) by Philip Campbell and Jason Stamp, published August 2004, and available at URL http://www.sandia.gov/scada/documents/sand_2004_4233.pdf

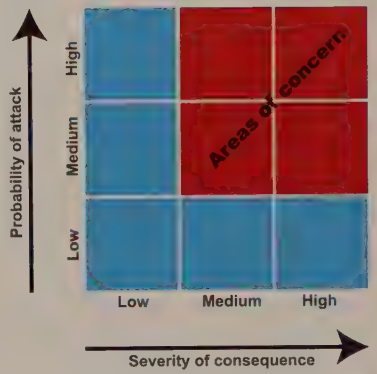
In general, the following simple conceptual equation can be used to quantitatively rank vulnerabilities:

Risk = (existence of unmitigated **V**ulnerability [1 or 0]) *
(**P**robability of Threat to exploit vulnerability [0-1]) *
(**C**onsequence of successful exploitation [cost])

Total risk of a system would be the sum of individual risks:
Total Risk = Sum [Vi * P(Ti) * Ci]

Reducing any of the three factors reduces the risk.

Another way to assess risk is using the high-low method. The consequence and probability of each vulnerability are estimated as high, medium, or low. Those vulnerabilities rated as medium or above in both categories are of highest concern.



# Security Documentation

Who:

Manager

Engineer/Tech

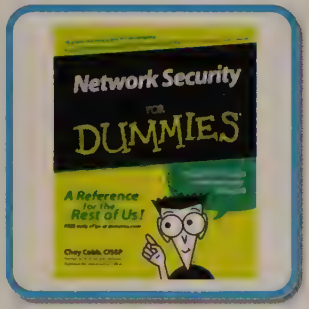
Security Admin

Why: Having the right documentation is a crucial part of securing your system over the long haul. This section describes the different elements needed for documenting the security of a system. It also provides guidelines for developing the security documentation.

What:
- Security Documentation Introduction
- Documentation Relationships
- Types of Security Documentation
- Security Plan Elements
- Implementation Guidance

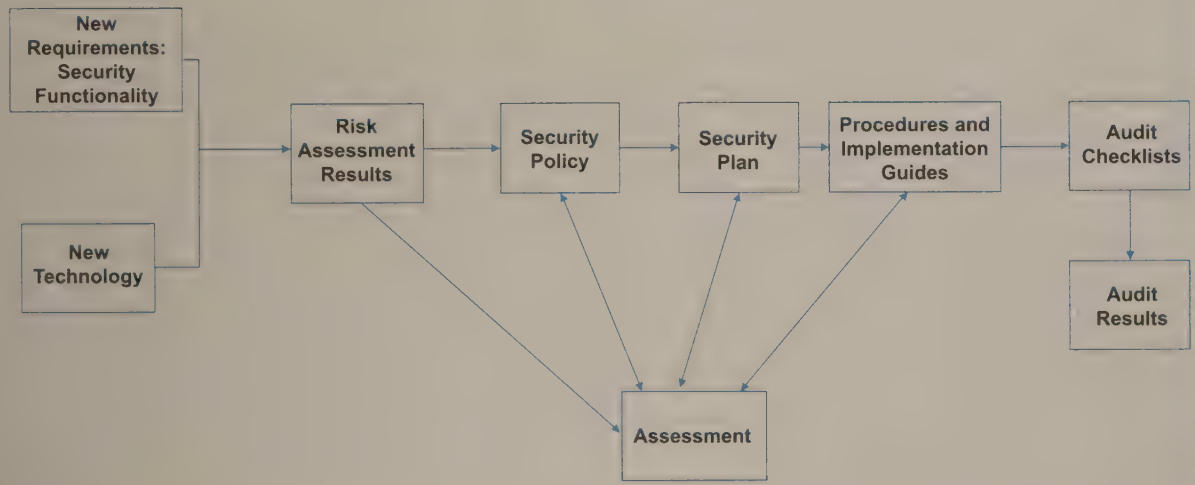
# Security Documentation Introduction

- Proper documentation is crucial to system security over the long haul.
  - o Security policy
  - o Security plan
  - o Implementation guidance
- Security documentation must be taken seriously and fully enforced.
  - o Without enforcement documentation is useless.
- Personnel must be fully educated in all relevant security documentation.
  - o Staff must be aware of policies and be willing to enforce them.



## Documentation Relationships

This flowchart illustrates the relationship between documents. The chart also shows how documents build upon each other. This is not a timeline for when documentation should be written.



## Types of Security Documentation

Security Policy

- A security policy for ICS administration translates security and reliability objectives into a set of rules and expected behaviors for system users.
- Security policy is covered in more depth in the Policy section of this guidebook.
- Security policy is the root document of any sustainable security program; it directs the staff toward designing, implementing, and operating a reliable and secure ICS.

21

See Policy

NERC

Procedures

- Procedures document appropriate behavior for repeatable situations. Incident response procedures, and evacuation procedures, are examples of typical procedures needed by ICSs. Implementation guides are a subset of procedure documents.
- Procedures documents give users step-by-step instructions on performing tasks in the system. If audits uncover that procedures are not being followed, the security team must investigate why and either update the procedures or implement training to ensure that users understand what necessitates the procedures. Some critical procedures are discussed in the **Incident Handling and Response** section of this guidebook.

# Types of Security Documentation (cont.)

Security Plans

- The ICS security plan documents the process of planning and maintaining adequate, cost-effective security protection for a system.
- The security plan provides an overview of the security requirements of the system and describes expected security controls in the system, as well as the responsibilities and proper behavior of any individual who might access the system. The security plan is created by both management and personnel as a practical guide for following the requirements of the security policy in the actual system.

NRC
API
http://

Implementation Guidance

- Implementation guidance enforces the security plan and policy. Implementation guidance is a set of directives for the installation, configuration, and maintenance of specific technologies.

## Security Plan Elements

- System identification
  - o System name
  - o Responsible organizations
  - o Contact information
  - o System owners
  - o Security personnel
  - o Operational status (e.g., design, development, operational)
  - o Description of the system
    - Purpose
    - Software
    - Hardware
  - o Operating environment
    - Details that drive security decisions
  - o Current network diagrams
  - o Relevant laws
  - o Relevant regulations
  - o Relevant policies
  - o Sensitivity
- Management controls
  - o Audit/assessment management
    - Dates
    - Results
  - o Audit/assessment results
    - Dates for necessary changes
  - o Rules of Behavior
  - o Accreditation
  - o Lifecycle planning
- Operational controls
  - o Personnel security
  - o Physical access
  - o Emergency preparedness
    - Contingency plans
    - Manual operations plans
  - o Data protection
  - o Security training
  - o Incident response
- Technical controls
  - o Access controls (e.g., passwords, smartcards)
  - o Logging requirements

# Implementation Guidance

- Implementation guidance enforces the security plan and policy for the implementation of specific technologies.
- Implementation guides explain how to configure, use, maintain, and retire any equipment used in the system.
    - o One improperly managed component can make a whole system insecure.
- Each version of every piece of equipment made by any vendor needs its own implementation guide.
- Implementation guides must be updated when one of the following occur:
    - o New technology is integrated into the system.
    - o Relevant new vulnerabilities are announced.
    - o New patches become available.
    - o Configurations change.
- Implementation guides should be very technical.
    - o Include step-by-step instructions for configuring and securing a component.
    - o Use strictly quantifiable standards so appropriate personnel can be audited for compliance.
- Audits are necessary to maintain compliance.
- If audits find that personnel regularly work around a security control, that security control should be replaced in the implementation guide.
- Implementation guidance is not optional.

NRC

API

# Policy

Who:

Manager

ISO

Security Admin

Why: The security policy is the root document of a security program. Without policy, there is no enforceable security in the system. A properly written and concise policy will remain usable over time.

What:
- Policy Introduction
- How to Write Policy
- What Goes into a Policy?
- ICS Security Policy Framework
- ICS Security Program
- Data Security Policy
- Platform Security Policy
- Communication Security Policy
- Personnel Security Policy
- Configuration Management Policy
- Audit Policy
- Application Policy
- Physical Security Policy
- Manual Operations Policy

*Sandeep Jolly, president of San Carlos, CA-based Jolly, Inc., a company that specializes in labeling and card software, claimed that in July 2004 an employee from the company's development center in Mumbai, India, uploaded source code and confidential design documents pertaining to a key Jolly product to her Yahoo e-mail account. Police investigating the incident said they had no indication that the employee transferred any documents from the computer in her office to any other location and therefore could not investigate further.*

*Police used technical experts in trying to uncover evidence of the file transfer, but claimed they were hindered by the Mumbai center's lack of a security policy. The facility "does not have a security policy. It has no log of the computer and network activity at the center, and passwords are known to all and sundry," said Vijay Mukhi, a technical consultant to the Mumbai police on this investigation. "We asked Jolly Technologies for the log, and they were unable to provide it to us," Mukhi added. "As the company has no log, I have no proof that there was a source code theft, and if so who did it."*

http://www.computerworld.com/printthis/2004/0,4814,95615,00.htm

## Policy Introduction

NERC

The security policy is the root document of a security program. It should include policies for the overall security risk management program, data security, platforms, communications, personnel, configuration management, auditing and assessing, computer applications, physical security, and manual operations. Each section of the policy defines the purpose, scope, positions, responsibilities, references, revision history, enforcement, and exceptions for a particular aspect of system security.

http://

Refer to example policies and templates on the TSWG website for further reference.

## How to Write Policy

Perform a risk assessment before writing a security policy. Once the security risks have been identified, policy can be written to mitigate them.

Identify the system data to determine what level of protection is required within the system.

Identify the data owners to ensure that there is a party responsible for implementing and enforcing the security policies.

Policy should be concise, not overwhelming.

## What Goes into a Policy?

**Purpose** Why this policy exists.

**Scope** What this policy covers (machines, people, facilities, etc.).

**Policy** Actual policy statements.

**Responsibilities** Who must do what in regard to this policy.

**References** Ties this policy back to other policies that must be followed due to organizational structure.

**Revision History** Past changes to this policy.

**Enforcement** Appropriate consequences for violating this policy.

**Exceptions** Exceptions, if any, must be documented in the policy.

### Good Policy Words

- Must
- Will
- Shall

### Bad Policy Words

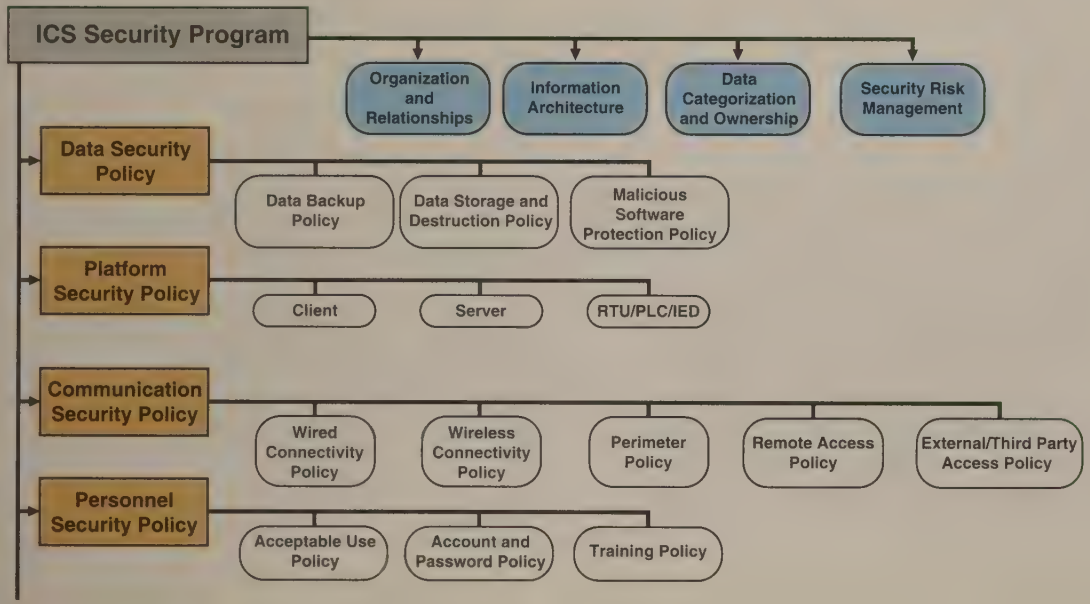
- Might
- Maybe
- Should

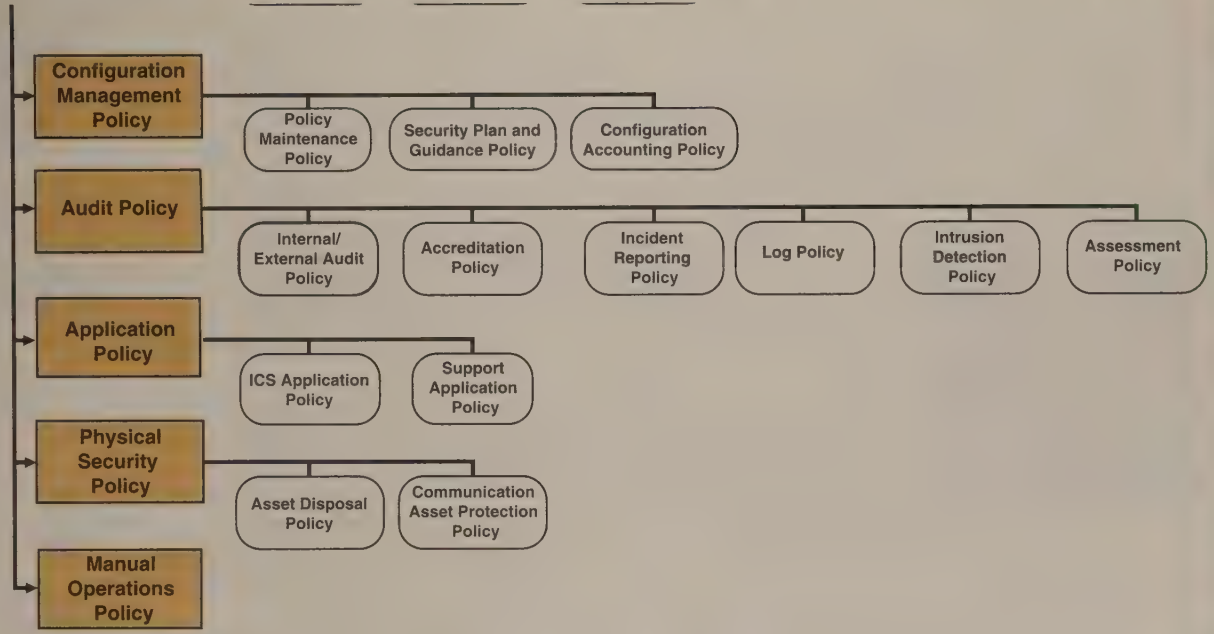
## ICS Security Policy Framework

The ICS Policy Framework makes creating ICS security policy easier:

- Authors can apply a systematic approach that ensures all critical topics have been adequately addressed by policy.
- Policies can be compartmentalized, allowing multiple authors to work at the same time with little or no overlap. Less overlap means that less work is required when changes must be made. Overlap can also lead to conflicting policy statements that reduce the effectiveness of the policy.
- The hierarchical nature of the framework allows the policy document to adapt to each organization using it.
- Particular policy sections that do not apply to an organization can be truncated or eliminated. New technology or procedures are not adequately covered by the policy because of missing sections, they cannot be used until the required policies are in place.
- Each box in the framework does not have to be a separate policy; some organizations will be able to cover every subsection in a policy area with one policy. Others may need the more distributed structure displayed.

# ICS Security Policy Framework




Configuration Management Policy
Policy Maintenance Policy
Security Plan and Guidance Policy
Configuration Accounting Policy
Audit Policy
Internal/ External Audit Policy
Accreditation Policy
Incident Reporting Policy
Log Policy
Intrusion Detection Policy
Assessment Policy
Application Policy
ICS Application Policy
Support Application Policy
Physical Security Policy
Asset Disposal Policy
Communication Asset Protection Policy
Manual Operations Policy

## ICS Security Program

- Introduces the target system and provides context for the rest of the policy.
- Provides important details and concepts necessary for the rest of the policy.

21

### Organization and Relationships

- Defines the organization and its relationship to other organizations.
- Relates the policy to other relevant policies.
- Defines the organization's hierarchy and reporting responsibilities.
- Gives roles and general responsibilities for individuals.
- Shows how a specific automation system relates critically to customers.

API

### Information Architecture

- Provides a common reference point for all readers of the policy.
- Defines the system boundaries and equipment.
- Identifies common terminology.
- Gives relevant engineering/performance standards.
- Describes each subsystem in terms of its relationship to other parts.
- Defines the architecture of the system to which this policy applies, as well as the design philosophy of that system.

## Data Categorization and Ownership

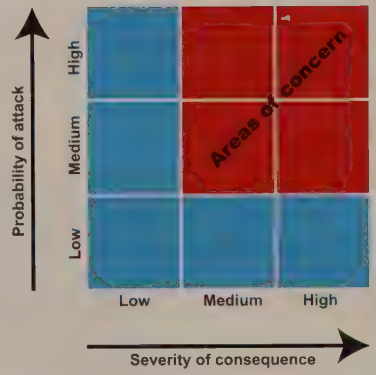
- Information regarding confidentiality, integrity, and availability requirements
- Types of information and functions performed on the information
- Data ownership

21

## Security Risk Management

- How corporate risk management applies to ICS
- Information about evaluating, reducing, and insuring against risk, as well as clarification of acceptable levels of risk

Risk = (existence of unmitigated Vulnerability)*
(Probability of Threat to exploit vulnerability) *
(Consequence of successful exploitation)




The total risk of a system would be the sum of individual risks:
Total Risk = Sum [Vi * P(Ti) * Ci]

Reducing any of the three factors reduces the risk.

Another way to assess risk is using the high-low method. The consequence and probability of each vulnerability are estimated as high, medium, or low. Those vulnerabilities rated as medium or above in both categories are of highest concern.

## Data Security Policy

- Specifies the treatment of the data categories defined in the security program.
- Protection of data in any form (paper, digital, video, etc.) should be commensurate with that data's criticality to the system.
- Provides data marking and need-to-know controls.

### Data Backup Policy

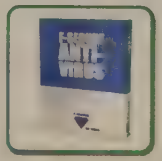
- Defines all of the details concerning what data must be backed up, how often backups must be made, and where the backups must be stored.
- Identifies retention schedule for backups.
- Identifies any exempt classes of devices.

### Data Storage and Destruction Policy

- Defines what must be done to protect data after it is no longer needed.
- Data must be protected during its complete lifecycle; creation, storage, and destruction. Destruction is as important as creation and storage, and it is often an adversary's easiest means of data theft.

### Malicious Software Protection Policy

- Controls that prevent inadvertent or intentional installation of any malicious code.



## Platform Security Policy

- Identifies secure configuration defaults required within the ICS.
- Addresses concepts such as virus checking, intrusion detection, access control, and encryption.
- A process for acquiring policy exceptions is necessary due to the differing capabilities of machines.

### Client, Server, RTU/PLC/IED

- Clients, servers, and ICS devices (RTUs/PLCs/IEDs) each require separate sets of rules for determining what defines a secure configuration.

## Communication Security Policy

- Identifies paths data take through the network and the level of protection necessary for each path.
- Identifies protection mechanisms for different network segments.
- Identifies security zones.
- Specifies external connection permissions.

### Wired Connectivity Policy

- Defines how to communicate within the wired portions of the ICS network, including all parts of the LAN, MAN, or WAN segments.
- Specifies cryptographic requirements based on data categorizations.

### Wireless Connectivity Policy

- Designates what type(s) of data may traverse the wireless network, and required cryptographic protections.
- Defines how connections to the network should be established.
- Approval process for wireless devices and processing.
- Identifies acceptable configurations for wireless connections to the wired network.
- Defines schedules and responsibilities for wireless coverage assessments.

## Communication Security Policy (cont.)

### Perimeter Policy

- Specifies data input and output from the ICS with other networks.
- Identifies the types of controls needed and the locations of these controls.
- Specifies security zones to determine the cryptographic controls needed.

### Remote Access Policy

- Defines whether and how users can connect to the ICS from remote locations.
- Specifies security controls needed for access control.
- Specifies minimum performance and security requirements for remote equipment.

### External/3rd Party Access Policy

- Specifies whether, when, and how outsiders can access information and equipment on the ICS network.
- Defines how to request access, who approves the access, and any time restrictions for access.
- Stipulates monitoring and logging requirements, prohibited actions, and other requirements.

## Personnel Security Policy

- Expresses job requirements and hiring policies for ICS staff (may include clearance, training, background investigation, etc.).
- Create termination procedures.

21

### Acceptable Use Policy

- Defines what users can and cannot do with equipment and network resources.
- Defines access to other networks and network monitoring requirements.

### Account and Password Policy

- Defines proper care of passwords and accounts, including storage, creation, and sharing.
- Defines special protections regarding creation, storage, and change requirements for shared passwords.
- Defines how users may use their accounts and who is responsible for creating and removing accounts.
- Defines additional protection requirements such as screen locks, timeouts, or login limits.

### Training Policy

- Lists what training is required, the frequency of training, and who must be trained.
- Lists any specialized training requirements needed by specific staff positions.
- Defines contractor training requirements.

## Configuration Management Policy

- Lists the necessary documentation and processes needed for sustainable security.

**Policy Maintenance Policy – Security Plan and Guidance Policy**

- Details the revision process and timelines for security plans, policies, and implementation guidance.

21

**Configuration Accounting Policy**

- Defines how equipment must be tracked.
- Defines elements of change control and change evaluation (including patching).

## Audit Policy

- Defines the scope of auditing and assessment activities.
- Identifies the individual(s) responsible for scheduling and reviewing audits.
- Delineates schedules for projected audits.

21

### Internal/External Audit Policy

- Details each type of audit.
- Identifies the internal organization responsible for performing the required audits.
- Identifies points of contact for external auditing.

### Accreditation Policy

- Details the responsible parties, timelines, and participating entities necessary for achieving accreditation or certification.
- NIST 800-37
    - Guidelines for the security certification and accreditation of federal information technology systems.
    - Though written for information systems, these guidelines may be a helpful start for developing accreditation policy for control systems.

## Audit Policy (cont.)

### Incident Reporting Policy

- Identifies responsibilities in the event of an incident.
- Identifies the chain of reporting.
- Identifies the protection level for incident details and reports.

### Log Policy

- Defines the requirements for what is logged.
- Defines storage requirements for log files.
- Defines the review and disposal schedule for log files.

### Intrusion Detection Policy

- Lists the requirements and limitations for IDSs.

### Assessment Policy

- Specifies the timelines, data protection needs, and parties responsible for assessments performed on the system.

## Application Policy

- Details application-level access control, data segregation, and application training requirements, as well as test and development requirements.
- Includes details for configuring and using applications in a manner commensurate with the security needs of the ICS.

### ICS Application Policy

- At times, ICS-specific applications require administrator-level access. These applications may also allow data separation, separate user logins, and password protections. This section focuses only on those applications written to interface with ICS devices and functionality.

### Support Application Policy

- Support applications such as office software, databases, and logging software need a different set of security guidelines. These applications usually do not interface directly with ICS equipment and automation functions, but may reside on the same PCs or networks where ICS applications are running.

## Physical Security Policy

- Defines physical controls and personnel and visitor access requirements.
- Defines behavior in emergency situations.
- Defines protection of mobile devices.

API

### Asset Disposal Policy

- Expresses requirements for disposal of physical assets no longer necessary for system operation.
- Defines sanitizing, tracking, and disposal methods.
- Defines special considerations for expendable media (CD, floppy, etc.).

### Communication Asset Protection Policy

- Communication equipment has different requirements from the standard office equipment used in the system. The differing characteristics of this equipment demand a separate statement of protection guidelines.

## Manual Operations Policy

- Due to the critical nature of automation systems, the functions of the automation system must still be performed even in the event of system failure.

- Recommended elements of a manual operations policy:
    - o manual backup procedures
    - o chain of command
    - o periodic inspection
    - o training in manual operations
    - o testing and drills for manual operating procedures
    - o disaster recovery

NERC

# Enforcement

Who:

Why: The most well-designed security program will still be ineffective if its provisions are not enforced. This section details some of the methods used to enforce security policies.

What:

- Enforcement Introduction
- The Enforcement Cycle
- Aspects of Enforcement
- Why is Configuration Management Necessary?
- Configuration Management: Step 1
- Configuration Management: Step 2
- Configuration Management: Step 3
- Changes
- Change Request/Approval Process
- Test Labs
- Essential Elements of a Test Lab
- Auditing Versus Assessment
- Types of Audit and Assessment
- Steps for Using Audit and Assessment Results
- What to Look for in an Assessment Company

*In March and April of 2000, on 46 separate occasions, Vitek Boden had complete control of the master control station that ran the Maroochy Shire, Queensland, Australia, waste management system. Boden had been employed by Hunter Watertech, the company that built the automation system, until a short time before several environmental attacks occurred. Commandeering the system was part of a plot he had hatched to maneuver himself into a position administering the system. During his months of control, Boden caused sewage releases into parks, rivers, and a resort hotel, blackening water, killing marine life, and leaving behind an unbearable stench for residents. In the end, Boden was only caught because a Hunter Watertech employee coincidentally decided to monitor system traffic while Boden was executing an attack.*

*In breaking in, Boden took advantage of the system's use of radio communication; he used a radio that operated in the correct frequency range and sent messages from his laptop that claimed he was "Pump Station 4." The messages were sent using automation system control software he had stolen from the facility (though at least three open-source programs would have done the job), and he provided authentication that had not been removed or updated since his firing.*

## Enforcement Introduction

The most well-designed security program will still be ineffective if its provisions are not enforced.

Human nature drives people to attempt circumventing policies restricting their actions if they do not believe in the objectives of those policies. This attempt can be caused by a desire to subvert the system or get the job done without the burden of the security steps.

A well thought-out enforcement program allows system engineers to save time and effort in maintaining the system, details the response process for when things go wrong, determines if the security controls remain effective, and punishes users who fail to follow regulations.

## The Enforcement Cycle

- The ICS security policy enforces the security and reliability needs of the company.
- Security plans and implementation guidance enforce the security policy.
- Configuration management enforces the security plan and implementation guidance.
- Auditing enforces configuration management, security plans, and implementation guidance.
- Overall, assessment (internal and external) enforces the entire chain of security.

# Aspects of Enforcement

NRC

Configuration Management

- Every component of the system must be identified and have its configuration data noted. Any change to a component must be controlled; configuration change must be a rigorously documented process. Configuration management is necessary for the entire lifecycle of both the system and its components; design, installation, and maintenance phases.

Auditing and Assessment

- The system must be periodically checked by both internal and external auditors and assessors ensure adherance to the documented policies, plans, and implementation guides, as well as its security.
- Assessments and audits are necessary for policy, and design, and implementation.
- Independent assessments
    - ensure that the security controls yield the right level of security,
    - are necessary because most internal assessors will have a hard time identifying their own oversights.

Monitoring and Logging

- They must be done in accordance with the risk assessment and the capabilities of the devices.
- This is an important tool for gauging policy compliance and effectiveness.

## Why is Configuration Management Necessary?

A well-designed configuration management program

- Saves both time and money.
- Allows staff to quickly determine what systems and equipment are at risk when a new vulnerability is identified.
- Allows staff to easily identify when equipment needs to be upgraded or replaced.
- Assists in disaster recovery by identifying lost or damaged equipment.

# Configuration Management: Step 1

**Identify what needs to be tracked and protected**

- Equipment
  - o Computers
  - o Network Devices
  - o RTUs, PLCs, IEDs
  - o Actuators and sensors
- Software
  - o Operating systems
  - o Applications (custom and commercial)
- Configuration Data
  - o Router configurations
  - o Firewall rules
  - o ACLs
- Documentation
  - o System diagrams
  - o Security controls

NERC

## Configuration Management: Step 2

**Develop the baseline configuration**

- Collect all relevant information: versions, patch levels, model numbers, operating system, firewall rules, router configurations, RTU settings, etc.
- Outfit every device with a unique identifier; make sure this identifier is visible on the device. This will assist staff in determining the device's configuration.

## Configuration Management: Step 3

**Track changes**

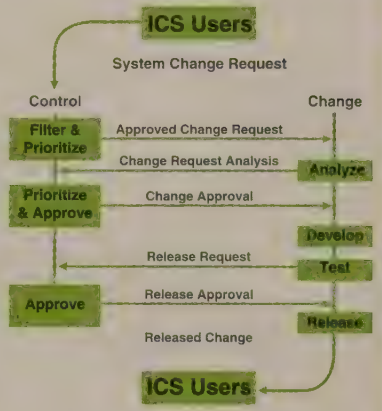
- Systems evolve over time.
- Changes must be recorded; records must include who made the changes, what was changed, and why the change was made.
- Any change to the system must be vetted on a test system before being introduced to the production system. This prevents system crashes resulting from incompatible upgrades.
- Develop procedures for testing and verifying changes.

## Changes

There are many types of changes: operating system or software upgrades, new hardware, new users, application changes, etc.

Each change requires a different level of change control.

Adding a new user may not require a full approval process, but adding new software should.




## Change Request/Approval Process

Optional for some changes, critical for others

- Changing equipment without approval could be disastrous.
- Adding a new user to the system may not need approval.

Change approval requires a written, well-known process in order to be effective.

## Test Labs

How can you be sure that a newly issued patch will work for your system? You need to test, in a realistic environment; testing on an ideal network that does not adequately represent your system is a waste of time.

A development environment with all the important common elements of the actual system should be employed to test new patches, antivirus updates, software, etc., before introducing these changes into a live environment.

Procedures must be developed to implement changes in the manner that has the smallest operational impact on users and systems.

## Essential Elements of a Test Lab

An ideal test lab would be an exact replica of the entire system.

A realistic test lab should include:

- Workstations and servers running every operating system used in the real system.
- A sample of the network equipment (a router, a switch, a firewall, etc.).
- One of each type of PLC, RTU, sensor, etc., employed in the real system.
- Some representative system data (old data captures work well).

Data must be similar to what the organization will collect/use/process on a day-to-day basis.

Configure all software and equipment as an accurate representation of the actual system.

## Auditing Versus Assessment

API

21

http://

Auditing

- Enforces configuration management, security plans, and implementation guidance by verifying their proper use.
- Uses checklists and guidelines (e.g., Windows XP Security Checklist, NIST guidelines).
- Is used to determine if the system is following best practices in security; also can be used to determine if system is following its own policy.
- Must be done periodically; frequency should be specified in the security policy.

Assessment

- Enforces the entire chain of security administration,
- Determines whether the controls in place are sufficient to secure the system,
- Evaluates the threats and risks specific to the system,
- Develops policy, security plans, etc.,
- Often best to have an external assessment so the system can get a fresh look by experts in the field.

# Types of Audit and Assessment

Types of audits

- Conformance Audit
  - o Does the system conform to documented policy?
  - o Is the system configured as documented?
  - o Is the system set up according to best practices?
- Physical and Cyber Security Audit
  - o Does the system follow security best practices?

Types of assessments

- Threat Assessment
  - o Identify threats to the system, both internal and external.
- Vulnerability Assessment
  - o Identify the system's vulnerabilities in its normal operating environment, assigning a weight to each vulnerability to establish its priority.
- Risk Assessment
  - o Identify vulnerabilities that can and should be fixed immediately and provide a starting point for disaster recovery planning for risks that cannot be fixed.
- Red Team Assessment
  - o Identify high-consequence vulnerabilities, modeling adversaries of interest.

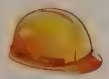
## Steps for Using Audit and Assessment Results

1) Protect the audit/assessment report
   - This document is a roadmap of the security protections and weaknesses of a system, and, as such, is invaluable for an attacker. This information must be protected at the highest level to prevent inadvertent disclosure. For example:
     - o When transmitted over the Internet, use encryption.
     - o Lock up hard copies.
     - o Encrypt copies stored on network drives.
2) Read the report
   - All the time, effort, and money spent on an assessment/audit are wasted if the final report is never read. If the report generated by an external firm is not conducive to reading (e.g., a 200-page output from a penetration test), ask the company for an executive summary of the most critical necessary improvements.
3) Take action
   - Determine the critical changes that must be implemented and schedule these first. After the most critical fixes are in place, generate a schedule for the other fixes and make sure to follow it.
4) Follow up
   - Once a certain percentage of the fixes are implemented, a follow-up assessment should be performed to ensure that the fixes were implemented properly and had the desired effect on security.

## What to Look for in an Assessment Company

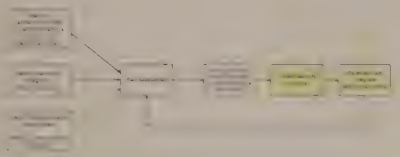
- Reputation
  - o Look for an assessment company with a reputation for providing useful feedback, serving customers responsibly, and being trustworthy.
- Non-Disclosure Agreements
  - o Make sure the assessment company is willing to sign a non-disclosure agreement. This is critical for keeping the system's vulnerabilities under wraps.
- History of Protecting Results
  - o Find an assessment company with a reputation for keeping results confidential. Leaked assessment results could easily result in complete penetration of the system.
- References
  - o References can include past customers as well as trusted third-party certification companies.
- Experience
  - o Assessment experience will give an assessor a good idea of what to look for when assessing your system; an assessor who is familiar with systems similar to yours might add some unique domain knowledge to the assessment.

# ICS Best Practices



Following best practices allows systems teams to benefit from the knowledge and experience of others. This section will list best practice recommendations for designing, building, and maintaining a secure ICS.

The best practices section follows the same general order as the policy framework. This format ensures that all the points covered in policy are also covered by technology. The Enforcement section of this guide has more detailed coverage of configuration management, so it will not be covered here.



**Secure Design Process**

*On May 11, 2001, security engineers at the California Independent System Operator, a nonprofit organization essential to managing the state's electricity flow, discovered that hackers had infiltrated parts of their network. According to the LA Times, the agency estimated that the attacks had gone undetected for 17 days. Some familiar with the attack claimed that the hackers almost gained access to "key parts of the system," which would have allowed them to cause state-wide disruptions in electricity. The attacks were traced to servers in Santa Clara, CA, Tulsa, OK, and the Guangdong province of China, but the attackers' actual locations remain unknown.*

*The systems the attackers gained access to were at Cal-ISO headquarters in Folsom, CA, and were linked to the system that controls electricity flow. Attackers took advantage of machines that were not behind a firewall, had no intrusion detection capability, and were misconfigured to leave open many more ports than were necessary. After the attack was discovered, investigators found that the attackers had been trying to compile code on Cal-ISO systems that could potentially have given them access to more secure parts of the network.*

http://archives.openflows.org/electronetwork-l/msg00013.html

## Defense in Depth

21

Defense in depth (also referred to as multi-layer security) is the practice of incorporating layers of security so that the breach of any single layer does not result in the complete compromise of the system. For example, access control types can be combined so that John Doe (user-based) can only access a resource from a certain host or network (host-based) during normal business hours (time-based). Another example is that if an adversary compromises a site's physical security, integrity checks and encryption of the data would still protect the integrity and confidentiality of the data.

## Security Program Best Practices

NERC

- Design security and functionality to match business needs.
- Establish an ICS security policy.
- Train operators and personnel in security awareness.
- Assign dedicated security responsibility.
- Perform risk assessments to prioritize and drive the security design process.
    - o Perform audits to verify that security design and implementation mitigate identified risks to an acceptable level.
    - o Mitigate risks to acceptable levels by using best practices and proven risk-reducing mechanisms.
- Include security concerns in RFQs and purchasing decisions.
- Implement security enclaves consistent with data sensitivity.
    - o Never violate security enclaves.
- Do not use the Internet for transport of real-time control or deterministic/critical data communications.

## Policy Best Practices

- Evaluate exceptions to policies annually.
- Make policy readable for the intended audience; users must be able to understand what they are required to follow.
- Policy should be technology-neutral.

## Organizational Best Practices

- Develop a security architecture.
    - o Architecture is specific to the ICS mission; the architecture must provide secure and reliable storage, processing, and transmission of system data.
    - o Architecture is designed to implement the security policy.
- Perform system and network management away from the ICS communications, or protect system and network management functions using encryption and strong authentication.
- Separate the control system from the corporate system.
- Limit communication between the control and data hierarchy; keep the data separate from the control functions.
- Eliminate global access/privilege requirements.
    - o Use the principle of least privilege.
    - o Implement need-to-know restrictions.
- Set access level commensurate to level of data sensitivity.

## Best Practices for Data Security

- Implement need-to-know information and access control for data.
- Use encryption to protect data.
- Data backup
    - Store backup tapes in off site storage facilities.
    - Make daily incremental backups.
    - Make weekly full backups.
    - Exercise backups periodically to ensure that the backup process is working correctly and data can be restored.
- Data storage
    - Protect data during storage according to its classification level (this may mean a locked room, safe, etc.).
    - Mark data with the appropriate categorization.
- Data destruction
    - Destroy secret or classified data completely using shredding, degaussing, or physical destruction.
    - Use approved wiping software to erase confidential or proprietary information.

## Best Practices for Malicious Software Protection

- Only system administrators may install software.
- No personal use on ICS equipment.
- No user should be given administrator privileges unnecessarily.
- Email should not be allowed on ICS.

21

Authorization:

- Restrict execution privileges for programs.
- Access controls
  - o Strong passwords
  - o Cryptographically secure password storage
  - o Secure remote authorization (e.g., radius server)
  - o Authentication and encryption for RTUs, PLCs, and IEDs where appropriate and available
- Decide which services are necessary
  - o DHCP, SSH, Telnet, FTP, TFTP, BOOTP, SMTP, SNMP, HTTP, etc.
  - o Disallow in-band remote management.
  - o Consider file sharing carefully.
  - o Security of networked operating systems (NOSs) is complex.

## Best Practices for Platform Security (cont.)

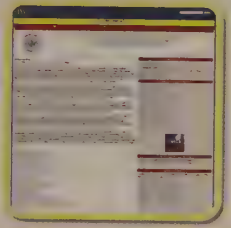
Logging

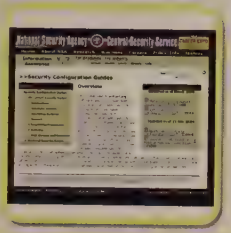
- Log remote and local connections.
- Review system and IDS logs for anomalies or attacks.
- Determine appropriate retention periods.
- Ensure that logging policy meets standards and requirements.

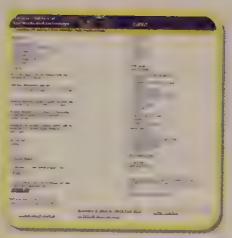
All systems should have current host firewall and malicious code protection software installed and running if possible.

Resources

- SANS guides: http://www.sans.org/
- NSA guides: http://www.nsa.gov/snac/
- NIST guides: http://csrc.nist.gov/publications/nistpubs/
- GOVCERT: http://www.us-cert.gov/





## Security for RTUs, PLCs, IEDs, etc.

21

Security requirements

- Develop as strong and effective a password policy for ICS equipment as possible.
  - o Use physical controls and ACLs to supplement equipment's inadequate security capabilities.
- Tightly control remote configuration for ICS equipment. Employ authentication and access controls when available.
- Develop strong and effective physical security for RTU equipment.

Security workarounds

- Use protocol gateways with security checks.
- Use terminal servers for access.
- Change passwords often.
- Increase physical security (e.g., cameras, doors, locks, guards, guns).

## Best Practices for Communication Security

NERC

- Identify the electronic security perimeter.
- Protect each part of the network from the other parts of the network.
- Ingress/egress point security includes firewalls, filters, and IDSs.
- Use antivirus checking with updated antivirus signatures.
  - o Test all AV solutions and updates to ensure that the solution will not negatively impact reliability.

## Best Practices for Wireless Security

- Avoid using wireless, especially for critical communication or sensitive data.
- Use strong encryption on all wireless traffic.
- Employ MAC filtering to restrict access to the wireless network.
- Disable SSID broadcasts.
- Use obscure SSIDs that will not identify an access point as belonging to your company.
- Employ war-driving techniques to test the system security.
- Limit RF coverage to ensure that only the area necessary for the wireless network can access the wireless network.
- Monitor access attempts to the wireless network.

## Best Practices for Virtual Private Networks

A Virtual Private Network (VPN) is any technology that allows the sharing of network resources over an insecure channel. VPN products achieve confidentiality using encryption techniques.

- VPN encryption should be reviewed annually and configured for the protection required.
- When necessary, strong authentication should be required to initiate a VPN.

## Best Practices for Firewalls

The purpose of a firewall is to prevent unwanted packets from entering or leaving a network. A properly configured firewall will close off all unnecessary inbound and outbound ports; if it is stateful it will only allow incoming packets that are part of a previously allowed traffic flow.

- Firewalls should be deployed between connected networks with different need-to-know requirements.
- Firewalls should be deployed between critical ICS networks and more vulnerable business intranets or the Internet.
- Specific access control lists (ACL) should be created for each firewall in accordance with ICS security policy.
- Security measures and access controls should be verified through audit, with additional testing to ensure that the firewall defaults to a reasonably restricted or secure condition after reset or failure.
- Services requiring external connections should use data transfer points, DMZ, or proxies.
- All data paths must be approved.
- All access through firewalls must be approved.
- No direct connections should be allowed through the firewall in either direction; use DMZs.
- Firewalls should be configured to allow only necessary data to pass through. Ports should be closed by default; only open those necessary for functioning.

## Best Practices for Demilitarized Zones

Demilitarized zones (DMZs) serve to prevent direct connections between devices inside the firewall and devices outside the firewall. A DMZ is an extranet that forms a buffer between the inner network and the outer network. When implemented correctly, a DMZ can be compromised without allowing any threats through to the inner network.

- Do not allow hosts in the DMZ to initiate connections out of the DMZ.
- Connections may be established from the outer network to the DMZ.
- Connections may be established from the inner network to the DMZ.
- Hosts residing on DMZs will be configured as Bastion Hosts.

## Best Practices for Proxies

A proxy is an intermediary system that acts as both a server and a client for the purpose of making requests on behalf of other clients. Proxies are often used as client-side portals (i.e., agents that can access the Internet on behalf of clients) through the network firewall and as helper applications for handling requests via protocols not implemented by the client application.

- Configure proxies to hide internal client information (e.g., IP address).
- Log connection information for security review.

## Best Practices for Remote Access

NERC 21

- Any type of remote access to the system must be approved, managed, monitored, and secured.
- Authorized remote access by external parties must follow stringent guidelines, requiring administrators to allow and disallow access and to be notified of connects and disconnects.
- Unused and unapproved remote access must be removed.
- Access may be disabled by physically disconnecting the device or by disabling remote access services.
- Protection mechanisms
    - o Positive ID for authorization.
    - o Authenticate user/device.
    - o Token cards/one-time passwords.
    - o Encrypt traffic.
    - o Log all usage.
    - o Use access timeouts and lockouts, activity timeouts, and time-restricted access.
    - o Principle of least privilege.
    - o Deactivate when unnecessary.

## Best Practices for External or Third Party Access

21

- Make sure there is a valid reason to give access to the third party.
- Allow external vendors access through protected mechanisms only, including
    - Authentication
    - Access controls
    - Application proxies
    - Minimum privilege
    - Deactivate when not in use or unnecessary
- External sources of data
    - Application proxies and validity checking
    - Procedures for operation when receiving invalid data
    - Receive as analog
- Providing data to external systems
    - Use archived data
    - View-only terminals

## Best Practices for Remote Access Servers (RAS)

A remote access server is a device that handles multiple incoming connections from remote users who need access to central ICS resources. Remote access can be established via dial-up modems or broadband Internet connections.

- Remote access servers should reside on a DMZ or on the outside firewall interface.
- One-time passwords should be used for initial authentication.
- Encryption should be used to protect additional authentication and data communications.
- The RAS used to allow remote access should be a dedicated ICS device and should not be used for other applications.
- Split tunneling should be disabled on this machine.
- Remote access clients should have current host firewall and malicious code protection software installed and running.

## Best Practices for Personnel Security

- Due to the criticality of the ICS, only ICS business should be allowed on ICS equipment.
- Personal and non-ICS work should not be performed on the ICS.
- Software on the ICS should be ICS-specific.
- Create a "rules of behavior" document that every employee is required to read and sign.

## Best Practices for Accounts and Passwords

- Minimize use of shared accounts and passwords.
- Use banners to identify systems and give warnings regarding company policy (e.g., company use only, or monitoring).
- Accounts
    - Accounts must be individually assigned based on job function. This allows for accountability and employs the principle of least privilege.
    - Disable default administrator and guest accounts.
    - Remove unused and unneeded accounts.
    - Lock accounts after a small number of concurrent failed log-in attempts. The number of attempts allowed must be tested to ensure that unnecessary lock-outs do not occur.
- Passwords
    - Protect passwords based on the criticality level of the data they allow access to.
    - Ensure that password rules require memorable passwords while avoiding guessable passwords.
        - Passwords should be comprised of a combination of upper and lower case letters, numbers, and special characters.
        - Using phrases can make passwords more memorable and stronger.
    - Passwords should not include user names, company names, or standalone English (or other common language) words.

## Best Practices for Training

NERC 21

Train all users before granting access to systems.

- All users must be retrained annually.
- Ensure that contractor training is comparable to internal staff training.
- Keep users up-to-date on security using newsletters, memos, and e-mails.
- Training should include
  - o Security policy
  - o Physical/electronic access controls
  - o Acceptable use guidelines
  - o Data protection
  - o Incident reporting
  - o Manual operations plan
  - o Continuity of operations plan
  - o Change control/configuration management

## What to Look for In a Training Class

- Reputation of the company.
- Examine lesson plans to ensure that training is appropriate and contains the correct level of information.
- Trainers and developers of the class should be practitioners; they must be able to explain and implement what they teach.

## Best Practices for Assessment

- Always perform an assessment when adding new features or upgrading the system.
- Periodic assessments should be performed to manage risk.
- Penetration test assessments should not be performed on live ICSs. This type of active testing can cause unforeseen consequences; therefore, passive tests are always preferred on live systems.
- Active testing should only be performed on the test system.

## Best Practices for Auditing

- A baseline audit should be performed before starting a security program. This audit measures the current state of security for a system.
- Use follow-up audits to show compliance after security changes have been implemented.
- Periodic audits are necessary to ensure that security goals are being met and that security controls are being implemented and followed.
- Always perform an audit when security documentation is changed.
- Perform an audit when new security requirements are mandated.
- Perform an audit when new technology is added to the system.

## Best Practices for Intrusion Detection Systems

Intrusion detection systems (IDSs) attempt to detect attacks by looking either for anomalous network or file system behavior or by trying to match network traffic patterns to known attack signatures. Host-based IDSs (HIDSs) look for malicious incoming connections and changes to important system files, while Network-based IDSs (NIDSs) comb incoming network traffic for potential attacks.

- Update IDS signatures as new signatures are developed; always test updates in the test lab.
- Tune anomaly-detecting IDSs to acceptable alert levels.
- Enable real-time alerting capabilities for critical events.
- Do not enable IDS automatic response without extensive, thorough testing to ensure that common, unusual, and emergency situations will not cause reliability problems.
- A network IDS should be placed between the firewall and the private network.
- HIDS:
    - Test HIDS with ICS functionality before deploying on operational systems.
- NIDS:
    - Test NIDS with ICS functionality before deploying on operational systems.
    - Deploy NIDS at network choke points, such as firewalls.
    - Use a switch that does not throttle bandwidth to the maximum speed of the Switch Port Analyzer (SPAN). This will limit the amount of traffic the NIDS sees, but it will also allow the ICS network to continue running at normal speed.

## Best Practices for Intrusion Prevention Systems

Intrusion prevention systems (IPSs) build on IDS capability by adding the ability to prevent an attack from being successful. IPS systems can be signature-based, blocking only well-known, and well-defined attacks, or anomaly-based, inferring that abnormal traffic patterns might represent attacks.

- Do not enable IPS to automatically block traffic on ICS networks without extensive testing in the test lab for all situations: common, unusual, emergency, and incident response.
- Use anomaly detection for notification purposes only.
- Use an IPS between the business and ICS networks if mission critical data does not travel between the two.

## Best Practices for Logging

- Store logs in write-protected files.
- Write logs to a dedicated, centralized, protected server.
- Review logs in a timely manner.
- Inspect logs before they are overwritten by later logs if rotating logs are used.
- Be aware of time criticality and storage requirements.

## Best Practices for Applications

Ensure that applications are configured and used in a manner commensurate with the security needs of the ICS.

- ICS applications
  - o Consider security options when evaluating vendor applications
  - o Activate application-level security options
    - Application-level access control
    - Cryptography
    - User and event logging
- Support applications
  - o Do not install unnecessary applications on ICS computers.

## Best Practices for Manual Operations

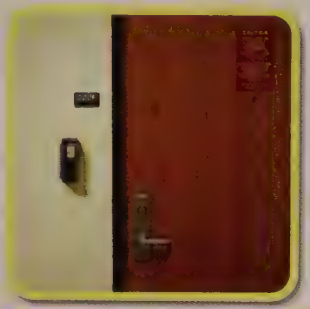
- Ensure that all critical functions can be performed in the event of an ICS failure.
- Test manual operations procedures at least once per year.
- Train all new staff in manual operation procedures.
- Inspect manual operating capabilities whenever upgrading.

## Best Practices for Physical Protection

NERC

21

- Control rooms and other rooms with critical equipment must have lockable doors installed.
- Control rooms should not have windows through which the room can be viewed from insecure areas.
- Close and secure all doors.
- If constant surveillance is needed in a specific area, apply a two-person rule.
- If immediate access to a computer is critical, there should be no need for screen locks because the control room should never be unattended.
- Protect equipment used by the ICS from physical damage, unauthorized access, and unauthorized destruction.
- Control and monitor visitor and personnel access to any equipment.
- Conduct surveys of local and remote sites to identify perimeter and risks.



## Best Practices for Physical Protection (cont.)

Networking equipment

- must be in an access-controlled room,
- may only be accessed by necessary and authorized personnel.

Wireless communication

- Test wireless links.
- Develop comprehensive wireless signal maps.
- Keep current on the latest standards and developments (very dynamic industry).

Cable/fiber communication

- Check cable/fiber for possible wire taps.
- If possible, protect all communication lines from physical access.
- Physically secure distribution and patch panels.

## Best Practices for Physical Asset Disposal

NRC

- Inspect all physical equipment before releasing it from the control of the system owners.
    - For rewritable media, including hard drives, floppy disks, CD-RW, and zip drives, remove identifying labels and use wiping software to remove all data.
    - Write-once media should be physically destroyed.
- Check drawers of file cabinets and desks to ensure that nothing has been left behind.
- Examine flat surfaces to ensure that paperwork (e.g., rosters, organizational charts) is not attached.

## Other Security Suggestions

- Implementation guidance should mandate secure default configurations on all network and computing devices.
- Force strong passwords and eliminate default passwords.
- Disable in-band management (e.g., SNMP, Telnet, FTP/TFTP, web) protocols.
- Disable finger.
- Disable routing of unused address space; maintain routing entries for necessary address spaces only.
- Use ACLs to ensure that all traffic travels along approved paths.
- Control switch and hub connections.
- Disable unused ports and services.

## Finding Your Vulnerabilities

**Who:**

Security Admin

Operator

**Why:** Understanding the existing vulnerabilities of ICS technology is critical when deciding how to implement security.

**What:**
Vulnerabilities and Threats
ICS Security
Poor ICS Practices
Lack of ICS Security Documentation and Enforcement
Lack of Physical Controls
Inadequate Physical Protection of Equipment
Remote Access
Types of Remote Access
Lack of Data Categorization and Sensitivity Guidance
Protocol Vulnerabilities

*In January 2003, when the SQL Slammer worm began hitting networks around the world, users of the business network at Ohio's Davis-Besse nuclear power plant began to notice a network slowdown. The worm spread from the business network to the operations network, causing enough congestion to crash the computerized panel used to monitor the plant's most crucial safety indicators. Minutes later, the Plant Process Computer, another monitoring system, crashed as well.*

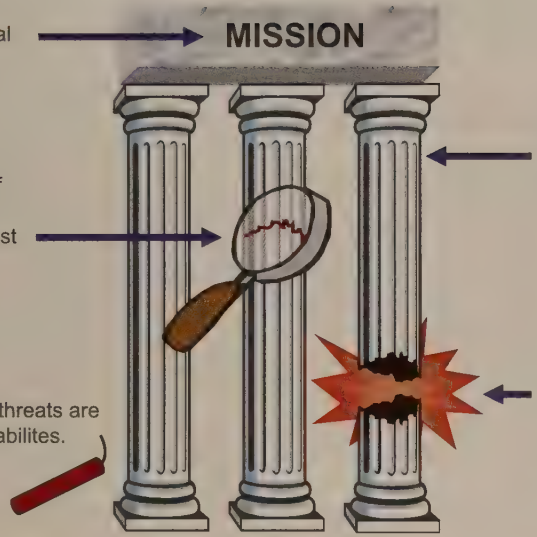
*The plant's firewall blocked Slammer, but the worm still managed to spread to the plant because of a T1 connection to an unsecured contractor's network. Had the plant's operations network been properly protected from either the contractor's network or the plant's own business network, or had the plant operators installed Microsoft's patch to prevent the Slammer infection (released 6 months earlier), the infiltration would have been avoided.*

*The incident luckily did not result in disaster because the plant was off-line for maintenance at the time of infection, and the crashed monitors were being backed-up by analog counterparts. Still, the incident serves as a warning of the potential consequences of low security.*

http://www.securityfocus.com/news/6767

# Vulnerabilities and Threats

Purpose and Direction, critical to Organization's success.




## Vulnerabilities

Weaknesses of Assets that if exploited devalue the Asset. Vulnerabilities will always exist in any system.

## Threats

Reveal Vulnerabilites; cyber threats are largely characterized by capabilites.

## Assets

Resources contributing to organization achieving its Mission. Assets may be tangible and intangible.

## Events

Can exploit a revealed Vulnerability.

- Attacks
- Natural Events
- Carelessness
- Malfunctions

# ICS Security

**Historical ICS Security**

- In past years, ICS networks were standalone systems in which most communication employed proprietary, relatively unknown protocols.
- Security issues were not considered a great concern because there were limited interactions with outside systems coupled with proprietary communications.

**Current issues**

- Newer ICS implementations are being developed (or updated) using the outdated assumptions that held true years ago: isolated networks, obscure protocols, no potential attackers, and low visibility.
- Higher visibility in recent years and the increasing use of modern information technology (IT) components, due to vendor product improvements and more complex business needs, contribute to increased risk.
- When industries adopt low-cost communication technology (e.g., IP networks, Internet communication, Windows) they also adopt the accompanying vulnerabilities and threats.
- Increased attention to critical infrastructure has revealed vulnerabilities to cyber attacks, which is garnering the attention of attackers.
- Strong evidence indicates terrorist organizations are specifically targeting critical infrastructure operations through both physical and cyber means.

**Security limitations of legacy equipment**

- Not developed with security in mind.
- No user accounts.
- No logging.
- Typically lack encryption.
- Usually a single privilege level.
- Passwords must be chosen from a small set of characters.
- Password length tightly limited.
- Inability to deactivate unneeded network services.

## Poor ICS Practices

### Poor Account Maintenance

- All users have administrative access.
- Users share the same account.
- Weak, publicized, or blank passwords.
- No account logins.
- Minimal access control.
- Accounts are not updated or removed when they become unnecessary.
- Account usage is not logged.

### Unprotected Network Connections

- Connections to administrative or other networks and services.
- Unencrypted connections over vulnerable or shared links.
- Unidentified critical monitoring and control paths.
- Single points of failure.
- Insecure wireless connections.
- Lack of rogue wireless detection.

### Poor Application Implementation

- Lack of development environment or testbed.
- Patches not tested.
- New software not tested.

## Poor ICS Practices (cont.)

**Lack of Maintenance and Monitoring**

- Operating system security patches is not maintained.
- Virus protection software is not maintained.
- Firewall and router software is not maintained.
- Security logs are turned off or unexamined.
- ICS network is left unmonitored.
- Default operating system configurations used.

## Lack of ICS Security Documentation and Enforcement

**Problem:** *Security documentation, including policy, security plans, and implementation guides, is incomplete or missing. Existing security controls are not enforced.*

*This key vulnerability allows the proliferation of procedural and technical vulnerabilities.*

**Solution:** Systems without sustainable security policy and administration do not possess measurable, self-perpetuating security; experience has shown that any ungoverned information network will sprout vulnerabilities.

## Lack of Physical Controls

**Problem:** *Physical Controls are not properly implemented when they are used as alternatives to cyber protections.*

- Cyber-security controls (e.g., passwords, screen locks) are not used because the physical location of the devices is secured.
- A common argument against passwords is that the control room doors are always locked and/or attended.
    - A common observance in these same locations is that the doors to the control room are propped open to increase airflow or allow easy access.

**Solution:** If physical security is determined to be the protection mechanism for any part of a facility, controls must be implemented correctly and practiced constantly:

- Doors must not be propped open.
- If constant surveillance is needed in a specific area, a two-person rule must apply (everyone has to take a break at some point).
- If immediate access to a computer is critical, then screen locks are not necessary as the control room should never be unattended.

## Inadequate Physical Protection of Equipment

**Problem:** *Protection of networking equipment is overlooked.*
**Solution:** Network equipment must be in an access-controlled room, and only authorized personnel may access the room.

**Problem:** *Wireless links are not tested or secured.*
**Solution:** Test all wireless links to develop comprehensive wireless coverage maps.

**Problem:** *Cable/fiber connections are never inspected for physical intrusion. Unused/spare network connections are unknown or unprotected.*
**Solution:** Check cable/fiber for possible wire taps. If possible, protect all communication from physical access.

## Remote Access

**Problem:** *Authentication for remote access is substandard, ad hoc, or nonexistent. Remote access into the ICS network uses shared passwords and shared accounts.*

**Solution:** Authenticate users/devices using individual accounts and strong passwords. Use try counters to prevent password guessing.

# Types of Remote Access

Types of remote access

- Third party
  - Contractors
  - Maintenance personnel
- Vendors
- System integrators
- Remote management
- Remote operators

Requirements for remote access create different levels of risk and request from different business needs. Extreme care should be taken to grant access to remote parties only when absolutely necessary. Remote access capabilities should be removed when the need for access no longer exists.

Controls on remote access

- Contractual agreements with liability for damages caused by third party access.
- Establish links to system only during periods when actual work is performed.
- Maintain and monitor logs for remote access accounts.

## Lack of Data Categorization and Sensitivity Guidance

**Problem:** *When there is no guidance as to what data to protect and at what level, breaches of security are predictable. Users of the system will inadvertently release or discuss information that, when publicly known, will pose a risk to the ICS.*

**Solution:** Without clear guidance regarding the sensitivity of data, it is impossible to know what to protect and at what level.

Absence of these fundamental distinctions makes it impractical and fruitless to identify where security precautions are appropriate (e.g., which communication links to secure, or which databases require protection).

The system owner must identify what data are used in the ICS.

## Protocol Vulnerabilities

**Problem:** *Protocol implementations lead to possible vulnerabilities. Protocols rarely include authentication, encryption, or integrity checking.*

**Solution:** Length fields should be used to determine message information. If a piece of data does not conform to proper length, data may be misread, applications may fault and crash, or buffer overflows can occur.

Integrity checking (when included) is weak.

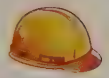
# Incident Handling and Response

**Who:**

Manager

Security Admin

Operator


Engineer/Tech

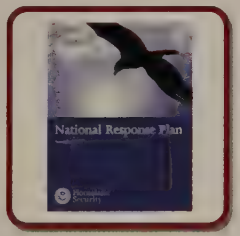
**Why:** All systems, no matter how secure, must have plans in place to respond to unusual situations, threats, and cyber-incidents. Without such plans, incidents of unnecessary downtime, data loss, equipment loss, etc., may occur.

**What:** How to Recover When Something Goes Wrong
Incident Handling
Incident Handling Process
After The Fact
Indications of Incidents
What to Do About Unusual Activity
Malicious Code Resources
Hoax Investigation Sites
Detection Investigation Sites
Digital Forensics
Threat Response

# How to Recover When Something Goes Wrong

Develop response guidelines

- Response guidelines are step-by-step instructions on how to recover from some type of event
  - o Natural disasters
  - o System and equipment failures
  - o Cyber intrusions
- Response guidelines should be regularly reviewed and exercised.
- Key Response Guidelines
  - o A Manual Operations Guideline is key for ICSs, as it ensures that ICS staff can perform critical ICS functions manually.
  - o Incident Handling Guidelines detail reporting requirements, backup recovery procedures, and underestimation procedures.
  - o Continuity of Operations Guidelines define procedures for failing over to backup systems and, when primary systems come back online, failing back to the primary systems.



## Incident Handling

What do you do when you discover something has gone wrong? Without a documented incident-handling procedure, critical information could be lost. This information is critical in determining what went wrong, the results, and who the perpetrators are.

What to consider

- Criticality of systems (what can be touched, what cannot)
- Acceptable downtime
- Fail-safe procedures
- Notification (whom to notify and when)
- Backup and recovery

NRC

# The Incident Handling Process

NERC

The incident handling process ensures that systems suffer minimal downtime and that evidence is retained for possible prosecution. It also gives investigators sufficient time to properly examine the incident. It is important to document all steps taken when responding to an incident.

**Wait** - Do not immediately run to fix the problem.

- You might make it worse (e.g., cut off users).
- You will destroy evidence.

**Preserve and backup** - Make copies of all relevant logs and of images of any affected machines.

- Allows more time to investigate later.
- Provides more evidence for the prosecution.
- Use write-once media to ensure integrity. Digitally sign images if write-once media is not an option.
- Make multiple copies if possible.
- A forensics toolkit may help for this step.

**Notify** - Do not attempt to find and punish the perpetrators. Have procedures for whom to contact and when.

- System administrator
- Security staff
- Law enforcement
- Users (maybe)

## The Incident Handling Process (cont.)

**Lock down** - Secure the affected system

- May require severing network connections.
- May require wiping the system and reinstalling from the baseline (see Configuration Management).
- Use the backup system in the interim.

**Investigate** - Investigate the logs and system images.

## After The Fact

After the immediate goal of restoring the system has been accomplished, investigate the root cause of the incident. Without determining why an incident happened, the likelihood of the same incident or a similar one occurring again is high. Root causes for security incidents include

- Improperly configured equipment
- Lack of security training or understanding
- Employees working around inappropriate security controls

Once the root causes are identified, policy, plan, or procedure changes may be necessary to prevent future incidents. Review the incident documentation to see if the incident response procedure worked smoothly and efficiently. Use this review to determine if the process can be improved.

## Indications of Incidents

Network

- IDS/IPS alert.
- Network performance degrades.
- Increased number of user issues.
- Abnormal internet activity, particularly machines trying to make unexpected network connections.
- Accounts are being used at unusual times.
- Accounts are attempting to access unusual resources.

System

- Computer runs slower.
- Hard drive activity light flashes constantly, indicating constant activity.
- Systems run out of disk space.
- Unknown programs or processes running.
- New files appear; existing files change sizes.
- Unusual visual effects.
- Programs running unexpectedly.
- Start screens flash and disappear.
- Some programs no longer run, particularly security programs.
- System crashes or reboots unexpectedly.

## What to Do About Unusual Activity

Unusual activity may be discovered when reviewing log files. When this happens, steps must be taken to determine if the activity was an attack and what the results of the activity were.

- Examinethe logs in-depth.
    - o This allows investigators to determine the extent of the unusual activity.
- Complete forensic evaluation to determine if system files have been altered.
- If suspicious files or activities are revealed, take steps to clean the system and restore trust in system operation.

## Malicious Code Resources

F-Secure Computer Virus Info Center – http://www.f-secure.com/v-descs/
McAfee Virus Information Library – http://vil.mcafee.com/
Sophos Virus Information – http://www.sophos.com/virusinfo/
Symantec Antivirus Research Center – http://www.symantec.com/avcenter/
TrendMicro Virus Encyclopedia – http://www.trendmicro.com/vinfo/virusencyclo/
Virus Bulletin VGrep Database – http://www.virusbtn.com/resources/vgrep/

## Hoax Investigation Sites

Vmyths Hoax – http://www.vmyths.com/hoax.cfm
CIAC Hoaxbusters – http://hoaxbusters.ciac.org/

## Detection and Recovery Sites

Intruder Detection Checklist (UNIX) – http://www.us-cert.gov/reading_room/intruder_det_check.html
Recovering from a Trojan Horse or Virus – http://www.us-cert.gov/reading_room/trojan-recovery.pdf
Steps for Recovering from a UNIX or NT System Compromise –
http://www.us-cert.gov/reading_room/win_unix_system_comp.html

# Digital Forensics

Performing digital forensics of industrial control systems is similar to doing so on IT systems. Before the need arises, policy and procedures should be put in place to support this function. It is also important that ICS Engineers, Technicians, and Operators work with their vendors to identify the safest means of securing systems for forensic purposes.

Goals of a digital forensics policy:

1) Forensics procedures should support collection of information for possible prosecution.
2) Procedures should ensure collection of information that can help keep a situation from recurring.
3) Procedures should ensure that control system operation is not adversely affected.

Procedures should be defined to mitigate operational risk while mandating proper information collection to support other activities, including prosecution. Creation of a digital forensic tools disc and learning to use that disc are paramount to success.

If, as stipulated by policy, prosecution is a possibility, then creating a working relationship with local law enforcement officials is important. Specific steps necessary for evidence collection may differ by locality.

## Digital Forensics (cont.)

Each incident needing forensic examination is likely to be unique. Procedures should be flexible enough to ensure that important information is not destroyed or lost during forensics exams. Below is a general procedure for the initial forensic investigation. This procedure is used for components of the system that contain general purpose computers, not PLCs or RTUs. Tools to perform forensic analysis on PLCs or RTUs do not currently exist.

1) Determine if system is critical to operation. Can it be shut off temporarily? Can it be replaced with a live spare or replaced with another system?
2) If the system is up, use a forensic tools disc if possible to image volatile data, such as memory. If the system is down, do not power it up; remove the power cord from the back of the system.
3) If the system is up, shut it down by removing the power plug from the back of the computer (do not just unplug the system from the wall outlet, as some systems have UPS connections). Do not use system commands to shut the system down.
4) Create verifiable images of all of the system's disk drives.
5) If the system was networked, identify disk storage it used on other systems and create verifiable images of those disks as well.

## Threat Response

Planning and preparation are key to responding to threats, be they environmental (e.g., hurricane or flood) or malicious (e.g., bomb threat).

- Notification plans
  - Employee notification
  - Emergency response or law enforcement notification
- Mission critical personnel
  - People crucial to the continued operation of the system
  - Last to leave and first to re-enter in the event of evacuation
- Evacuation plans
  - Detail how to evacuate staff and in what order
  - Identify and publish evacuation routes
- Search procedures
  - Searches may be necessary depending on the nature of the threat
  - Current maps and floor plans make searching more efficient
- Continuity plans
  - Plans for continued critical operation in event of an emergency

## Section 1: Start Here


1. TSWG SCADA Security website
   http://www.tswg.gov/tswg/ip/scada.htm
2. "21 Steps to Improve Cyber Security of SCADA Networks"
   http://www.tswg.gov/tswg/ip/21_Steps_SCADA.pdf
3. NERC Critical Infrastructure Protection Standards CIP-002-1 through CIP-009-1
   http://www.nerc.com/~filez/standards-cyber.html
   http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html
4. "AGA-12: Cryptographic Protection of SCADA Communications General Recommendations"
   http://www.gastechnology.org/webroot/downloads/en/1ResearchCap/1_1GasOps/AGASCADANews.pdf
5. "NRC: Criteria for use of Computers in Safety Systems of Nuclear Power Plants"
   http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-152/
6. API's "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries" and "Security Guidelines for the Petroleum Industry"
   http://www.npra.org/publications/general/SVA_2nd_Edition.pdf

## Section 2: Setting the Foundation


1. HIPAA (Health Insurance Portability and Accountability Act of 1996)
   http://www.cms.hhs.gov/hipaa/
2. Gramm-Leach-Bliley Act
   http://www.ftc.gov/privacy/glbact/
3. Federal Information Security management Act (FISMA)
   http://csrc.nist.gov/sec-cert/
4. California Senate Bill 1386
   http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
5. National Strategy to Secure CyberSpace
   http://www.whitehouse.gov/pcipb/
6. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
   http://www.whitehouse.gov/pcipb/physical.html
7. The Freedom of Information Act (FOIA)
   http://www.usdoj.gov/04foia/
8. Stamp, Campbell, Depoy, Dillinger, Young. "Sustainable Security for Infrastructure SCADA," SAND2003-4670C
   http://www.sandia.gov/scada/documents.htm
9. AMWA. Atkins, Cathy and Morandi, Larry. "Protecting Water System Security Information." September 2003. - Summarizes applicable legislation and lists FOIA exemptions
   http://www.amwa.net/security/NCSL_FOIA.pdf

## Section 5: Policy

1. Kilman and Stamp. "Framework for SCADA Security Policy," SAND 2005-1002C
   http://www.sandia.gov/scada/documents.htm
2. SANS Security Policy Project
   http://www.sans.org/resources/policies/
3. CobIT Control Objectives for Information and related Technology
   http://www.isaca.org/cobit.htm
4. BS7799
   http://www.thewindow.to/bs7799/
5. Anecdote
   http://www.computerworld.com/printthis/2004/0,4814,95615,00.htm

## Section 6: Enforcement

1. API's "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries" and "Security Guidelines for the Petroleum Industry"
   http://www.npra.org/publications/general/SVA_2nd_Edition.pdf
2. Sandia National Laboratories. SCADA Assessment Training Course
   http://www.sandia.gov/scada/training_courses.htm

1. American Gas Association. AGA 12 - Cryptographic Protection of SCADA Communications General Recommendations. 2004
   http://www.gtiservices.org/security/AGA12Draft3r6.pdf
2. National Institute of Standards and Technology FIPS PUB 140-2 "Security Requirements for Cryptographic Modules"
   http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
3. SANS SCORE
   http://www.sans.org/score/
4. SANS/FBI Top 20
   http://www.sans.org/top20/
5. NIST – National Institute of Standards and Technology
   http://csrc.nist.gov/publications/nistpubs/
6. CobIT Control Objectives for Information and related Technology
   http://www.isaca.org/cobit.htm
7. BS7799
   http://www.thewindow.to/bs7799/
8. NSA Guidelines
   http://nsa2.www.conxion.com/support/download.htm
9. Anecdote
   http://archives.openflows.org/electronetwork-l/msg00013.html

## Section 8: Common Vulnerabilities

1. Stamp, Dillinger, Young, and Depoy. "Common Vulnerabilities in Critical Infrastructure Control Systems," SAND2003-1772C, May 2003
   http://www.sandia.gov/scada/documents.htm
2. Anecdote
   http://www.securityfocus.com/news/6767
3. FBI/SANS Top 20 Vulnerabilities
   http://www.sans.org/top20/

## Section 9: Incident Handling and Response

1. NIST 800-61 Computer Security Incident Handling Guide
   http://csrc.nist.gov/publications/nistpubs/
2. DOE EIA
   http://www.nerc.com/~dawg/append-a.html
3. F-Secure Computer Virus Info Center
   http://www.f-secure.com/v-descs/
4. McAfee Virus Information Library
   http://vil.mcafee.com/
5. Sophos Virus Information
   http://www.sophos.com/virusinfo/
6. Symantec AntiVirus Research Center
   http://www.symantec.com/avcenter/

## Section 9: Incident Handling and Response (cont.)


7. TrendMicro Virus Encyclopedia
   http://www.trendmicro.com/vinfo/virusencyclo/
8. Virus Bulletin VGrep Database
   http://www.virusbtn.com/resources/vgrep/
9. Vmyths Hoax
   http://www.vmyths.com/hoax.cfm
10. CIAC Hoaxbusters
    http://hoaxbusters.ciac.org/
11. DOE EIA
    http://www.nerc.com/~dawg/append-a.html
12. U.S. Department of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement:
    http://www.ncjrs.org/pdffiles1/nij/199408.pdf

# Resources

## Presidential Information

Homeland Security Presidential Directive on Critical Infrastructure: Identification, Prioritization, and Protection - HSPD-7
http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

Executive Order 13231: Critical Infrastructure Protection
http://www.fas.org/irp/offdocs/eo/eo-13231.htm

Presidential Decision Directive 63: Critical Infrastructure Protection
http://www.fas.org/irp/offdocs/pdd-63.htm

The National Strategy to Secure Cyberspace
http://www.whitehouse.gov/pcipb/

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
http://www.whitehouse.gov/pcipb/physical.html

## General Information

Cybersecurity for the Homeland DHS - December 2004
http://hsc.house.gov/files/cybersecurityreport12.06.04.pdf

Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors GAO - July 2004
http://www.gao.gov/cgi-bin/getrpt?GAO-04-780

## General Standards

System Protection Profile for Industrial Control Systems NIST
http://www.isd.mel.nist.gov/projects/processcontrol/

IT Security for Industrial Control Systems NIST and PCSRF
http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf

## General Guidance

21 Steps to Improve Cyber Security of SCADA Networks.
DOE and the President's Critical Infrastructure Protection Board
http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf

Common Vulnerabilities in Critical Infrastructure Control Systems. Sandia National Laboratories
http://www.ea.doe.gov/pdfs/vulnerabilities.pdf

Sustainable Security for Infrastructure SCADA. Sandia National Laboratories
http://www.sandia.gov/scada/documents/SustainableSecurity.pdf

## Applicable Laws

The Freedom of Information Act (FOIA)
http://www.usdoj.gov/04foia/

"CobiT Executive Summary," "CobiT Control Objectives," "CobiT Quickstart,"
http://www.isaca.org/cobit.htm

ISO-17799: Information Technology - Code of Practice for Information Security Management
http://www.iso-17799.com/

Threat Alert System and Cyber Response Guidelines for the Electricity Sector NERC and CIPAG
ftp://www.nerc.com/pub/sys/all_updl/cip/tas_cyber_v2.pdf

NERC CIPC Guides
http://www.nerc.com/~filez/cipfiles.html

NERC Urgent Action Standard 1200-Cyber Security
http://www.nerc.com/~filez/standards-cyber.html

NERC Urgent Action Standard 1300-Cyber Security
http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

FERC Security Standards for Electric Market Participants
http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=9538944

ISA-SP99, Manufacturing and Control Systems Security
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

## Definitions

**Access Control** - Any method or technology used to control which hosts and/or users have access to a given resource.

**Access Control List (ACL)** - A table used by the computer system to identify access rights for each user to a particular system resource, such as a file directory, an individual file, or a device. In networking, the term refers to a list of the computing services available on a server, each with a list of hosts permitted to use the service.

**Assets** - Resources contributing to an organization achieving its mission. Assets may be tangible or intangible.

**Authentication** - The process of verifying the identity of a user or process attempting to access systems or resources.

**Availability** - The assurance that authorized users can access the information necessary to complete their jobs.

**Bastion Host** - A gateway between an inside network and an outside network designed to defend against attacks aimed at the inside network.

**Classified** - Data that is not to be released outside of the organization; release could result in harm to the organization (and could harm national security).

**Company confidential** - Private company information; release could damage the company.

**Confidentiality** - Protects information against unauthorized access or disclosure.

**Configuration Management** - Enforces the security plan and implementation guidance.

**Cyber Security** - The protection of information system assets and data by all means necessary, including physical protections.

**DMZ (Demilitarized Zone)** - Security enclaves, usually located logically between the inside and outside interface at a firewall, also called extranets.

**Engineer/Technician** - Designs and maintains the ICS, participates in testing and designing security response guidelines (manual operations, incident response), maintains the system hardware.

**Event** - An action or occurrence that can exploit a vulnerability.

**Finger** - Displays information about a user or users on a specified remote computer (typically a computer running UNIX).

**For Official Use Only (FOUO)** - Unclassified information exempt from public release and restricted to need-to-know access.

**Implementation Guidance** - A set of directives for the configuration, installation, and maintenance of specific technologies.

**Information Security Officer** - Responsible for all data contained in the system, responsible for ensuring that security controls are adequate for the protection of data.

**In-Band** - The technique of transmitting controlling information over the same LAN the information is controlling.

**Integrity** - Ensures the correctness and appropriateness of a piece of information content.

**Intelligent Electronic Device (IED)** - Consolidates data from field devices.

**Link Encryption** - Encrypts data as it is transmitted between two hosts in a network.

**Manager** - Responsible for approving all changes to the ICS, exceptions to policy, purchasing, and new equipment; ensures all security requirements are met.

**Need-To-Know (NTK)** - The business requirement that allows an individual to only have access to and knowledge of specific, protected information necessary to fulfill their work duties.

**Operator** - Maintains the day-to-day operations of the ICS.

**Packet Encryption** - Encrypts data between two applications running on different hosts.

**Physical Security** - The protection of assets using physical devices and entities (such as guns, gates, and guards), allowing access only to authorized individuals.

**Principle of Least Privilege** - A user or process is given no more privilege than necessary to perform a job.

**Procedures** - Document appropriate behavior for repeatable situations.

**Programmable Logic Controller (PLC)** - Devices that provide hardware interface for input sensors and output actuators.

**Public** - Data is not sensitive; release of this information poses no threat.

**Reliability** - Ensures that users can depend on the information and resources of a system to be accurate and available when needed.

**Remote Access** - Any access to a device that originates outside of the system's network.

**Remote Access Server (RAS)** - A server that is dedicated to handling users not on a LAN but needing remote access to it.

**Remote Terminal Unit (RTU)** - Data interface between a control station and remote control equipment and field devices.

**Risk** - The possibility that a particular threat will exploit a vulnerability resulting in a consequence of concern.

**Risk Assessment** - The determination of risks and risk levels acceptable by a system. This type of assessment must take into account expected adversaries and their capabilities, as well as the vulnerabilities of the system.

**Security Administrator** - Maintains security documentation; oversees the implementation of all security controls; evaluates and implements the results of security audits and assessments; investigates security incidents; and administers users' accounts and application security.

**Security Enclave** - An enclave is the container for data elements of like security characteristics. Security enclaves can be implemented as perimeters or as access controls on storage media or platforms.

**Security Plan** - Enumerates security guidelines for systems, or groups of systems, based on fundamental concepts from the security policy.

**Security Policy** - Translates the desired security and reliability control objectives for the overall business into enforceable staff directions and behaviors to ensure secure ICS design, implementation, and operation. Security Policy bridges the control framework to enforcement.

**Single Point of Failure** - Any component of a system that upon failure will cause a malfunction in the entire system.

**Split Tunneling** - The process of allowing a remote VPN user to access a public network (most commonly the

Internet) at the same time that the user is allowed to access resources on the VPN.

**Threat** - A threat is a circumstance or event that can potentially cause harm to a system.

**Virtual Private Network (VPN)** - Any technology that allows confindential sharing of network resources across an insecure channel.

**Vulnerability** - A point of weakness in a system.

**Vulnerability Assessment** - The determination of possible security holes in a system. This type of assessment must take into account current technology and its possible uses and misuses.

**Wipe (wiping software)** - A method of removing data from electronic media. This method involves overwriting the existing data, usually multiple times.

| | |
|---|---|
| **ACL** | Access Control List |
| **AEPR** | Alarm and Event Processing Routine |
| **AES** | Advanced Encryption Standard |
| **AGC** | Automatic Generation Control |
| **AS** | Automation Systems |
| **AV** | Antivirus |
| **BOOTP** | Bootstrap Protocol |
| **CI** | Critical Infrastructures |
| **CM** | Configuration Management |
| **DCS** | Digital Control Systems |
| **DHS** | Department of Homeland Security |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DMZ** | Demilitarized Zone |
| **DoD** | Department of Defense |
| **EMS** | Energy Management Systems |
| **FIPS** | Federal Information Processing Standards |
| **FISMA** | Federal Information Security Management Act |

| | |
|---|---|
| FOIA | Freedom of Information Act |
| FOUO | For Official Use Only |
| FTP | File Transfer Protocol |
| HIDS | Host-based Intrusion Detection Systems |
| HIPAA | Health Insurance Portability and Accountability Act |
| HMI | Human Machine Interface |
| HTTP | Hypertext Transfer Protocol (world wide web protocol) |
| I/O | Input/Output |
| ICCP | Inter-Control Center Communications Protocol |
| ICS | Industrial Control Systems |
| IDS | Intrusion Detection System |
| IED | Intelligent Electronic Device |
| IP | Internet Protocol |
| ISAC | Information Sharing and Analysis Center |
| ISO | Independent System Operators |
| IT | Information Technology |
| LAN | Local Area Network |

| | |
|---|---|
| **MAC** | Media Access Control |
| **MAN** | Metropolitan Area Network |
| **NERC** | North American Electric Reliability Council |
| **NIDS** | Network-based Intrusion Detection System |
| **NIST** | National Institute of Standards and Technology |
| **NTK** | Need-To-Know |
| **PCS** | Process Control Systems |
| **PCSRF** | Process Control Security Requirements Forum |
| **PLC** | Programmable Logic Controller |
| **PX** | Power Exchange |
| **RAS** | Remote Access Services |
| **RF** | Radio Frequency |
| **RFQ** | Request for Quote |
| **RTO** | Regional Transmission Operator |
| **RTU** | Remote Terminal Unit |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SMTP** | Simple Mail Transfer Protocol (Internet email) |

Acronyms (cont.)

| | |
|---|---|
| **SNMP** | Simple Network Management Protocol |
| **SPAN** | Switch Port Analyzer |
| **SSID** | Service Set Identification (IEEE 802.11 wireless networks) |
| **SSH** | Secure Shell |
| **TCP** | Transmission Control Protocol |
| **TFTP** | Trivial File Transfer Protocol |
| **TSWG** | Technical Support Working Group |
| **UPS** | Uninterruptible Power Supply |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |
| **WAP** | Wide Area Protection |

## Standards and Association Links

### Broad Based Links

- Instrumentation, Systems, and Automation Society
  http://www.isa.org/
- National Association of Regulatory Utility Commissioners
  http://www.naruc.org/
- Sandia National Labs Center for SCADA Security
  http://www.sandia.gov/scada/home.htm
- Process Control Systems Forum (PCSF)
  http://www.pcsforum.org/
- NIST Process Control Security Requirements Forum (PCSRF)
  http://www.isd.mel.nist.gov/projects/processcontrol/

### Chemical Links

- Chemical Industry Data Exchange
  http://www.cidx.org/
- American Institute of Chemical Engineers
  http://www.aiche.org/

- North American Electric Reliability Council (NERC)
  http://www.nerc.com/
- Electric Power Research Institute
  http://www.epri.com/
- Office of Energy Assurance
  http://www.ea.doe.gov/
- Electricity Sector Information Sharing and Analysis Center
  http://www.esisac.com/
- International Council on Large Electric Utilities
  http://www.cigre.org/ -or- http://www.cigre-usnc.org/
- National Council on Electricity Policy:
  http://www.ncouncil.org/

- Energy Information Sharing and Analysis Center
  http://www.energyisac.com/
- American Public Power Association
  http://www.appanet.org/
- National Association of State Energy Officials
  http://www.naseo.org/

- National Center for Manufacturing Sciences
  http://www.ncms.org/

- Nuclear Regulatory Commission
  http://www.nrc.gov/

- Security Vulnerability Assessment Methodologies for the Petroleum and Petrochemical Industries API, May 2003
  http://api-ec.api.org/filelibrary/SVA_2003.pdf
- Security Guidelines for the Petroleum Industry - American Petroleum Institute
  http://api-ec.api.org/filelibrary/Security_Guidance2003.pdf

## Oil and Gas Links

- Gas Technology Institute (GTI)
  http://www.gastechnology.org/
- American Gas Association
  http://www.aga.org/
- American Petroleum Institute
  http://api-ec.api.org/
- National Petroleum Council
  http://www.npc.org/
- National Petrochemical & Refiners Association
  http://www.npra.org/

## Security Links

- Infragard
  http://www.infragard.net/
- Information System Security Association
  http://www.issa.org/
- Partnership for Critical Infrastructure Security
  http://www.pcis.org/
- Information Systems Audit and Control Association
  http://www.isaca.org/

## Water Links

- Water Information Sharing and Analysis Center
  http://www.waterisac.org/
- Association of Metropolitan Water Agencies
  http://www.amwa.net/
- American Public Works Association
  http://www.apwa.net/
- Water Quality Association
  http://www.wqa.org/
- Water Environment Federation
  http://www.wef.org/
- National Rural Water Association
  http://www.nrwa.org/
- Association of State Drinking Water Administrators
  http://www.asdwa.org/
- Ground Water Protection Council
  http://www.gwpc.org/
- Association of Metropolitan Sewage Agencies
  http://www.amsa-cleanwater.org/
- American Water Works Association
  http://www.awwa.org/

## ICS Primer

An ICS monitors and controls critical infrastructure equipment both locally and remotely. The system can be viewed as a collection of interconnecting devices and automated and human actions working together to monitor and control a particular infrastructure. The function and efficiency of an ICS depends on the types of equipment controlled and the communication methods employed by the ICS.

Local controls primarily protect equipment from damage by removing from service when set thresholds (temperature, pressure, current, etc.) are exceeded. Well-defined local control functions regulate and respond to system conditions within a specified range. Remote controls at control centers consolidate data from local equipment using automated and human actions.

## Two Categories of ICS

Control systems can be broken into two broad categories: those deployed in a single location, such as those used in manufacturing or chemical plants, and those spread out over multiple locations, such as those used in electric power, oil and gas, or water systems.

In the manufacturing and chemical industries, ethernet or modem networks typically transmit control data between local equipment and several distributed control areas or centralized control areas. These industries refer to ICSs as Process Control Systems (PCSs) or Distributed Control Systems (DCSs) rather than as Supervisory Control and Data Acquisition (SCADA) systems. A typical system has an interconnected network of programmable logic controllers (PLCs) and control centers that communicate via local area network (LAN) fibers or wires, supplemented with gateways and modems or serial lines to carry out the monitoring and control functions of the field devices. Because Ethernet is high-speed and the serial devices are relatively close to the PLCs, monitoring and control of devices can be very rapid.

In the electric power, oil and gas, and water infrastructures, ICSs have one or a few centralized control stations to communicate with a multitude of remote stations, each with a Remote Terminal Unit (RTU) or PLC to concentrate data from the remote station devices. The remote station connections can be as simple as an RTU connected with direct hardwires to panels and field devices, or a more modern configuration with RTU connections to serial or Ethernet intelligent electronic devices (IEDs) (which consolidate data from the field devices). RTUs, PLCs, and individual IEDs can also be Internet Protocol (IP) addressable, allowing for direct monitor and control.

- SCADA – Supervisory Control and Data Acquisition (All-encompassing government term for automation systems)
- EMS – Energy Management System
- Protection – Relaying
- AGC – Automatic Generation Control
- WAP – Wide Area Protection
- DMS – Distribution Management System

## Related Works in Progress

We refer readers to the future publication of NIST 800-82 – "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security" to be released as a public draft in September 2005 and as a final publication in January 2006. This publication may be found on the Internet at:

- NIST Special Publications: Computer Security Resource Center - CSD
  http://csrc.nist.gov/publications/nistpubs/

Additional resources that will be valuable for SCADA security may be found on the Internet at:

- NIST Process Control Security Requirements Forum (PCSRF)
  http://www.isd.mel.nist.gov/projects/processcontrol/

- Institute for Information Infrastructure Protection (The I3P)
  http://www.thei3p.org/

O9-CGE-779

**TSWG Mission:** Conduct the National Interagency Research and Development program for Combating Terrorism through rapid research, development and prototyping.

Please contact TSWG at ipsubgroup@TSWG.gov to provide comments or suggestions on this publication or to request further information on the TSWG and it's programs.

ISBN 978-0-16-075115-8

9 780160 751158 90000

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

ISBN 978-0-16-075115-8